4-2015

Joint Force Quarterly 77 (2nd Quarter, April 2015)

National Defense University Press

JFQ | Joint Force Quarterly

Issue 77, 2nd Quarter 2015

The Cyber "Domain" and Deterrence

Ethics of Big Data

Operational Leadership

Joint Force Quarterly

Founded in 1993 • Vol. 77, 2nd Quarter 2015

http://ndupress.ndu.edu

GEN Martin E. Dempsey, USA, Publisher
MajGen Frederick M. Padilla, USMC, President, NDU

Editor in Chief
Col William T. Eliason, USAF (Ret.), Ph.D.

Executive Editor
Jeffrey D. Smotherman, Ph.D.

Production Editor
John J. Church, D.M.A.

Internet Publications Editor
Joanna E. Seich

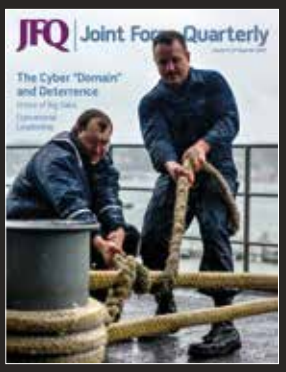
Copyeditor
Erin L. Sindle

Art Director
Marco Marchegiani, *U.S. Government Printing Office*

Printed in St. Louis, Missouri, by UNIVERSAL Printing Company

Cover 2 images (top to bottom): Retired Command Sergeant Major Bennie G. Adkins during press conference after receiving Medal of Honor at The White House, September 2014. In 1966, Adkins distinguished himself during 38 hours of close-combat fighting and 48 hours of escape and evasion, using mortars, machine guns, recoilless rifles, small arms, and hand grenades, killing 135–175 enemies and sustaining 18 wounds (U.S. Army/Bernardo Fuller); Marines with 24th MEU ashore in Kuwait as part of scheduled sustainment training post security during field training exercise (U.S. Marine Corps/Todd F. Michalek); Air Force wounded warrior August O'Neill and his service dog, Kai, at Nellis Air Force Base, where O'Neill competed in 6-mile handcycle heat with four others (U.S. Air Force/Jette Carr).

In this Issue



About the Cover
Sailors wrap line stopper around line on fantail of USS *John C. Stennis* (CVN 74), which is currently undergoing operational training period in preparation for future deployments (U.S. Navy/ Ignacio D. Perez)

Joint Force Quarterly is published by the National Defense University Press for the Chairman of the Joint Chiefs of Staff. *JFQ* is the Chairman's flagship joint military and security studies journal designed to inform members of the U.S. Armed Forces, allies, and other partners on joint and integrated operations; national security policy and strategy; efforts to combat terrorism; homeland security; and developments in training and joint professional military education to transform America's military and security apparatus to meet tomorrow's challenges better while protecting freedom today. All published articles have been vetted through a peer-review process and cleared by the Defense Office of Prepublication and Security Review.

NDU Press is the National Defense University's cross-component, professional military and academic publishing house.

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other agency of the Federal Government.

Submissions and Communications
JFQ welcomes submission of scholarly, independent research from members of the Armed Forces, security policymakers and shapers, defense analysts, academic specialists, and civilians from the United States and abroad. Submit articles for consideration by email to JFQ1@ndu.edu, with "Attention A&R Editor" in the subject line. Or write to:

Editor, *Joint Force Quarterly*
NDU Press
260 Fifth Avenue (Building 64, Room 2504)
Fort Lesley J. McNair
Washington, DC 20319

Telephone: (202) 685-4220/DSN 325
Email: JFQ1@ndu.edu
JFQ online: www.dtic.mil/doctrine/jfq/jfq.htm

2nd Quarter, April 2015
ISSN 1070-0692

Letter

To the Editor: In response to "Opportunities in Understanding China's Approach to the Senkaku/Diaoyu Islands" by Lieutenant Colonel Bradford John Davis, USA (*Joint Force Quarterly* 74 (4th Quarter 2014), I must argue against his proposal for joint patrols/resource development.

LTC Davis characterized the Senkaku Islands as "seemingly unimportant." If China were to occupy those islands, however, it would be able to extend its exclusive economic zone (EEZ) claim to the Okinawa Trough, and Japan's insistence on the Middle Line maritime boundary would lose legitimacy. Also, China's construction of intelligence facilities on the islands would create significant disadvantage for both the United States and Japan. I consider the Senkaku Islands to be a strategically important asset to check China's Pacific advance. When I was the director of Japan's Defense Intelligence Headquarters in 2004, a Chinese *Han*-class nuclear submarine intruded into Japanese territorial waters between Ishigaki and Miyako islands. The Senkaku Islands stand in the way of the People's Liberation Army (PLA) Navy's access to the Western Pacific.

Also, China's occupation of the Senkakus would strengthen its position toward Taiwan and put U.S. forces in Okinawa at risk. While LTC Davis wrote, "China and Japan can change their approach from the current win-lose dilemma into a win-win solution acceptable to both countries," I think the author's approach is naïve and discounts or ignores China's current "salami-slicing" strategy in the South China Sea. The United States should hedge with its strong ally, Japan, against Chinese expansion.

Second, Davis wrote, "Chinese fishermen used these islands as shelter and navigational aids back to the Ming Dynasty." He failed to mention the fact that fishermen of the Ryukyu (Okinawa) Kingdom also used the islands for the same purpose. He also failed to mention the fact that the Japanese government had surveyed and declared Senkaku Islands as its territory by cabinet decision in January 1895. Similarly, he failed to recognize that a Japanese dried bonito factory was established on the islands and that many Japanese had lived and worked there during World War II. He also omitted the very important point that China never claimed the Senkaku/Diaoyu Islands after 1895 until 1971, when the United Nations Economic Commission for Asia and the Far East announced the possibility of oil below the seabed in the area.

Third, the Senkaku Islands were part of the areas whose administrative rights were reverted to Japan in 1972 under the "Agreement Between the United States of America and Japan Concerning the Ryukyu Islands and the Daito Islands." The United States had used part of the Senkaku Islands as bombing and gunnery ranges until the mid-1980s. It is obvious that if the United States had recognized any Chinese sovereignty over the islands, it would not have used them as bombing and gunnery ranges. Therefore, the U.S. position over sovereignty should not be neutral.

Fourth, and most significant, the author put Japan and China on the same strategic level and recommended proposals such as joint patrols as well as joint resource development that ignore China's expansionistic and hegemonic intentions. Reports by both the Center for Strategic and Budgetary Assessments and RAND have stated that by 2020, China will be well on its way to having the means to achieve its first island chain policy.

The second island chain is composed of the Bonin Islands, Marianas Islands, Guam, and the Palau archipelago. China has noticed that this second island chain is scantily guarded in part because Japan's coast guard has augmented its presence in the Senkaku Islands in response to China's dispatch of over 200 red coral poaching ships in the waters surrounding the Bonin Islands, where they engaged in illegal resource exploitation in Japan's EEZ and territorial waters. Given the fact that red coral grows only 5 millimeters a year, we understand how China's willingness to ignore resource preservation makes joint resource development unrealistic.

In a 2012 publication, the PLA think tank Military Science Academy insisted that the PLA Navy must protect Chinese national interests west of 165° East and north of 35° South.

According to Alfred Thayer Mahan's *The Influence of Sea Power Upon History: 1660–1783*, translated by a Chinese scholar in 2004, the translator drew a three-line configuration including a third island chain, which included the Hawaiian Islands. We should remember that in 2012, members of a Chinese delegation reportedly suggested a potential People's Republic of China (PRC) claim to Hawaiian sovereignty to then–Secretary of State Hillary Clinton. Admiral Timothy Keating, then–commander of U.S. Pacific Command, was also reportedly approached in 2007 by a Chinese admiral with a plan to divide the Pacific into U.S. and PRC zones of influence. In 2013, Xi Jinping, general secretary of the Communist Party of China, stated to President Barack Obama that the vast Pacific Ocean has enough space for the two large countries of China and the United States.

The above indications demonstrate China's intentions to change the status quo. Japan does not possess such an ambition. Therefore, China is the status changer while Japan is the status quo power. That point is not clear in LTC Davis's article.

Last, but not least, China's *Global Times*—the international version of *People's Daily* by China's Communist Party—published an article on September 17, 2012, titled "China should implement her major power's responsibility to support the independence of Okinawa."

The article stated, "On March 4, 2006, there was a referendum in Okinawa. Seventy-five percent of people demand independence and recover free trade with China. The remaining 25 percent wanted to belong to Japan but agreed to autonomy." This article is completely fabricated and a typical example of China's media warfare. China's "Three Warfares Strategy" consists of media, psychological, and legal warfare. There was no referendum in Okinawa in 2006, and polling shows that a majority of people in Okinawa wants to remain part of Japan. In May 2013, *People's Daily* even discussed the legitimacy of PRC possession of Okinawa, where about 75 percent of U.S. sole-use bases in Japan are located. It is obvious that China is trying to drive a wedge between Japan and Okinawa.

Since Japan controls the Senkaku Islands, agreeing to the joint patrols/resource development would mark a significant Japanese retreat. If Japan concedes sovereignty over the Senkaku Islands as LTC Davis proposes, China will advance to claim the entire Okinawa Islands, expel U.S. bases, and may claim the Hawaiian Islands. Already these phenomena have been happening in the South China Sea. There is no international justice or legitimacy by ignoring these Chinese expansionistic and hegemonic intentions.

Finally, I would like to ask a question: Would the United States accept joint U.S.-PRC patrols and resource development of Hawaiian waters because China claimed territorial rights in Hawaii? Would that really be building a stronger diplomatic relationship based on strategic cooperation between Washington and Beijing, as LTC Davis's final statement about China and Japan suggests? If you do not think so, then you cannot support the author's proposal. JFQ

—Vice Admiral (Ret.)
Fumio Ota, Ph.D.

President Obama talks with General Dempsey after attending Armed Forces farewell tribute for Secretary Leon Panetta at Joint Base Myer–Henderson Hall (White House/Pete Souza)

From the Chairman
Defining Duty

Throughout over 40 years of service, I have maintained a list of principles to judge my actions against. Chief among these principles is duty. I have reflected and written on this topic throughout my career, and I strongly believe the concept of duty is central to the Profession of Arms. Indeed, it seems to me to be *the* cornerstone of the uncommon life to which we have dedicated ourselves.

Entrusted by society to apply violence on behalf of the Nation, we have a moral imperative to understand and uphold our solemnly sworn duty to "support and defend the Constitution." It is worth a conversation about what duty entails.

Our duty as Servicemembers resides in two primary responsibilities. First, we keep the Nation free from coercion. Second, we support our elected leaders as they perform their constitutional duties. To fulfill these responsibilities requires continued and lifelong development of three important traits: expertise, humility, and courage.

Expertise

Military leaders have a duty to understand the use—and the limitations—of the military instrument of power. We must be unrivaled experts in the application of force on behalf of the Nation.

At the tactical level, our teams and units require highly skilled leaders who accomplish their assigned missions with the greatest chance of success and minimal risk to the force. In this, we should always overmatch our adversary. To this end we must remain persistent students of the art and science of war, continually honing our skills as individuals, small teams, and units.

At the strategic level, civilian leaders depend on our advice and expertise to

General Dempsey presents Soldier with Bronze Star Medal during visit to Bagram Air Base, Afghanistan (DOD/Daniel Hinton)

assist in the development of national strategies consistent with our long-term national objectives. Our role is to offer options in discussions regarding the best use of military forces. We provide the "how we" and "can we" for any given situation, but we are not ultimately responsible for the "should we." That is, and always will be, a decision rightfully belonging to our elected leaders.

Our duty as military members is to accurately assess risks and present our best military advice with clarity and candor—whether planning a small unit–level attack or testifying about military posture before Congress. To fulfill these responsibilities, we must be trusted, and professional expertise is the necessary foundation of this trust.

Humility

Humility is the constant companion of expertise. Lifelong learning requires acknowledging gaps in our expertise, examining our successes *and* failures, and admitting both our strengths and weaknesses. This can be particularly challenging in a culture that prizes success and values immediately providing answers. Humility allows us to step back, set our ego aside, and embrace new ideas.

It takes humility to acknowledge that our civilian leaders do not have to accept our advice wholesale. Military leaders must have the humility to recognize that our senior leaders balance multiple competing demands. I can say with confidence that civilian leaders want to hear our advice. They know they owe it to the American people to consider all information and to weigh the risks before deciding on a particular course of action—and they take that obligation seriously.

For our part, we must recognize that the military is only one instrument in an array of national power. Frankly, it is often not the most important or appropriate instrument. In developing plans, policies, or budgets, there are always legitimate and competing considerations, and our civilian leaders are responsible to weigh and integrate these competing considerations. We must remember national security is but one aspect of a much larger set of choices.

Courage

Duty performed well requires courage. Certainly our line of work requires the physical courage to act in the face of grave bodily danger. Yet doing our duty also demands moral courage—that is, resolve in the face of ambiguity.

We intuitively understand acts of physical courage—honoring and rewarding those who display such acts. In praising these physical acts, we reinforce their importance to our concept of duty. It is not clear that we do the same to reinforce and cultivate moral courage. Duty may require us to advocate an unpopular position. It may require us to risk our personal ambitions. Duty may require the courage to act decisively or to show restraint.

In today's environment of ubiquitous communication, there is an inexorable pull to blog, tweet, comment, and post. Such media can host laudable professional expression, but some may be seduced by reading their name in print or receiving recognition online. Tempting as it may be to enter the limelight, we should consider that courage may require us to remain quiet professionals.

In policy development, disagreement is not disloyalty. Debate is healthy when conducted with professionalism and in the proper forums. But it is inappropriate to become a salesman for policy or to circumvent proper channels for discussion.

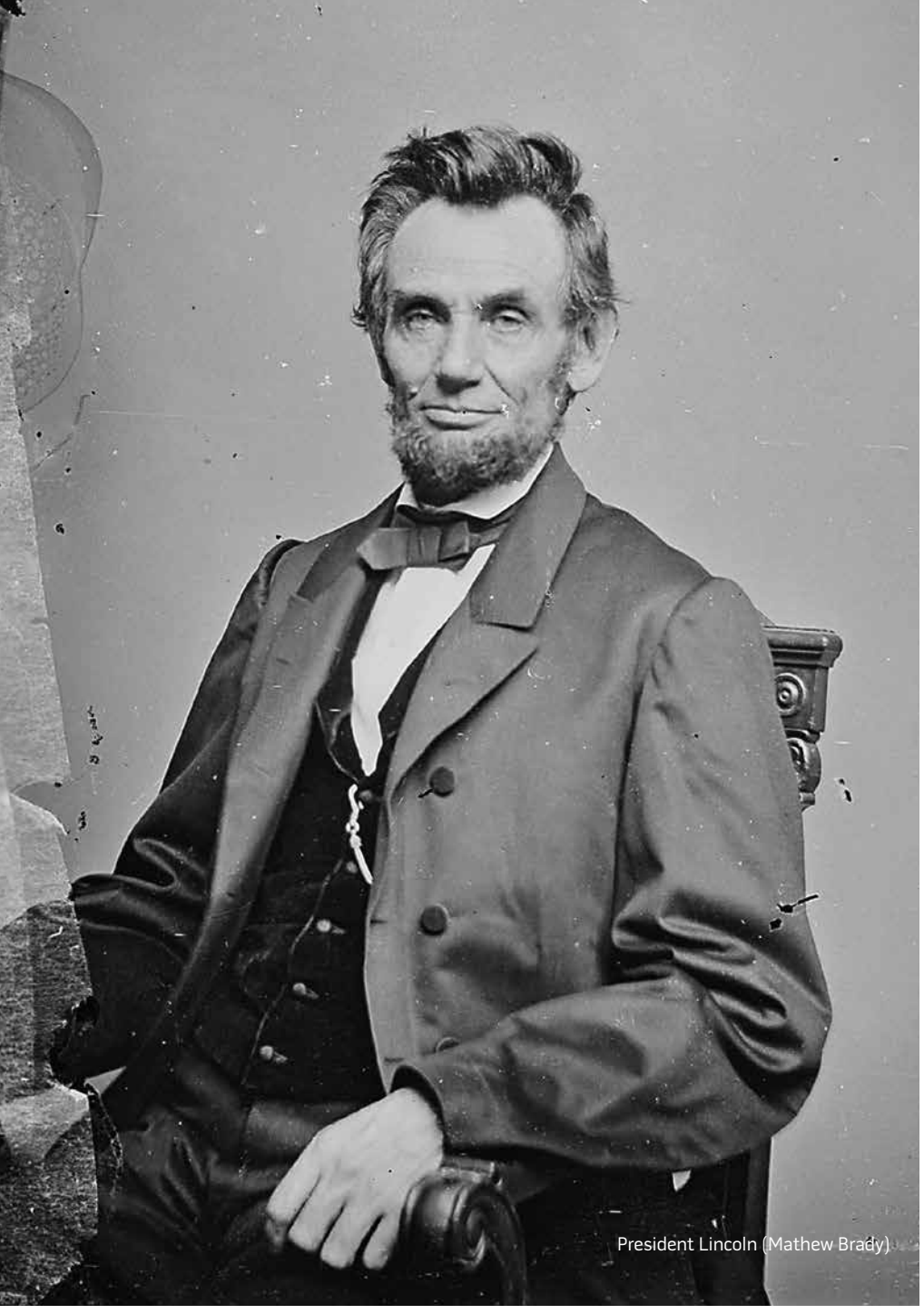
In the end, courage demands that we remain objective, unemotional, and apolitical.

An Uncommon Life

Clearly, a life devoted to duty—and the foundational traits of expertise, humility, and courage—is an uncommon life. Yet as Saint Augustine reminds us, "In doing what we ought we deserve no praise, because it is our duty."

Our commitment to a life of duty should give us no sense of superiority or entitlement but rather a deep sense of responsibility. Our duty as members of the military profession is an act of service best accomplished with a servant's soul. We must remember our military does not exist for its own sake. It exists for the Nation it serves. JFQ

Martin E. Dempsey
General, U.S. Army
Chairman of the Joint Chiefs of Staff



President Lincoln (Mathew Brady)

Executive Summary

A century and a half has passed since the end of the American Civil War and reminders both physical and cultural surround us, especially here in the Nation's capital. So let us reflect on one important idea of that time that today all Americans should consider, one that President Abraham Lincoln himself held in the front of his mind throughout the war: the value of seeking unity from diverse opinions. But what do we truly know about Lincoln's leadership skills? Actually, a great deal.

One book I find very insightful regarding his leadership is Doris Kearns Goodwin's 2005 *Team of Rivals.* Goodwin writes about Lincoln and his four main Republican rivals in the 1860 election, all of whom became members of his wartime Cabinet. Lincoln in time proved very masterful at understanding the Union's security environment during the war, even if his record shows he suffered through a series of less than effective generals who often did not seem to share his understanding. Probably the supreme example of Lincoln's understanding came during the Overland Campaign in May and June of 1864 when, despite incurring horrendous losses in Lieutenant General Ulysses S. Grant's forces in Virginia, the President decided to back Grant's campaign. He saw it as the only real option to exhaust Lee's army and remove the South's remaining military strength.

Surprise and uncertainty accompanied every turn of events in this war, but with each sign of bad fortune, Lincoln repeatedly summoned within himself an extraordinary amount of resiliency. From the losses early in the war to the death of his son, the President always weathered the storms of his personal and professional lives.

As the war wore on after Antietam, Lincoln saw an opportunity to seize the political initiative through his issuance of the Emancipation Proclamation, which packed the potential for a great amount of pushback on both sides of the conflict. After Gettysburg, he again saw the need for a change in leadership when he found "a general who can fight" in Grant.

From his efforts to understand and empower his political rivals around his cabinet table to work together for the common cause to his trust in Grant to lead the Union forces to victory, Lincoln demonstrated time and again a full command of the ability to operate on intent through trust, empowerment, and understanding. While this seems fairly obvious to most, the fact that these attributes are still what senior military leaders value some 150 years later speaks volumes about the measure of Lincoln as a leader, as well as the enduring nature of the human condition, especially in our most difficult situations.

In this edition of *JFQ*, our Forum section brings five very interesting views on issues we cannot actually see in a physical sense but are at the forefront of where defense strategists are working these days. Dorothy E. Denning leads with an important discussion of how cyberspace is far more like traditional domains of warfare than many have said previously, especially when considering strategy-related concepts like deterrence. Another area that is already having a big impact on society and the military is the use of "big data." A team of Joint Forces Staff College graduates, Karl F. Schneider, David S. Lyle, and Francis X. Murphy, provide us with a very useful essay on the ethical considerations of using big data in a military context. Chandler P. Atwood discusses how big data could be used to revolutionize intelligence analysis through a process called "activity-based intelligence" within the U.S. Air Force, and potentially across the joint force. Following the recent DOD Innovation Initiative announcement, Edie Williams and Alan R. Shaffer suggest that the prototyping of new capabilities can take the department to better solutions to emerging requirements. Cindy Hurst returns to the pages of *JFQ* with an assessment of the current and rapidly advancing state of Chinese computing and communications.

In JPME Today, Thomas P. Galvin suggests one method of enhancing the educational experience at the war colleges is to leverage an older practice that has fallen somewhat out of favor in some places: faculty papers written specifically for the courses the colleges teach. Taking us back in time in order to measure how far JPME has traveled, Anna T. Waggener compares the current education environment against the recommendations of the 1989 *Skelton Panel*, which set the bar for joint professional military education, and which she argues has had an obvious and positive impact on the achievement of successful joint combat operations in recent years. Advancing an important area of study for future joint leaders, Professor Milan Vego from the Naval War College returns with a valuable essay on operational leadership.

Technology and its impact on future combat is one theme of our Commentary section in this issue. Randy Eshelman and Douglas Derrick explore the impact of evolving artificial intelligence in machines on national security. Exploring the place of humans in wars of the future, Andrew Herr maps out the necessary arguments to consider as technology evolves at an ever-accelerated rate. Spoiler alert: we still matter, but there is a great deal to consider about how so. Another theme is how best to improve DOD's national crisis response as Richard Hayes takes us through a review of the Stafford Act as it relates to potential force deployments in our nation.

Our Features section brings us a range of issues to consider from geopolitical concerns in Northeast Asia and our military responses to considerations of operational leadership. Vincent A. Manzo, another *JFQ* alumnus, returns with his thoughts on what happens in Northeast Asia after the shooting starts. While Air-Sea Battle was the focus of intense discussions related to the Asia-Pacific shift strategy focus, Robert B. Brown and Jason N. Adler bring the land force contribution into focus as they discuss I Corps contribution to U.S. Pacific Command's operations and planning. Tyrone L. Groh and Richard J. Bailey offer their views on how to improve joint Phase Zero "shaping" operations through the application of a modified operational design process. A special operator by trade, Eugene Haase discusses the further development and value of the Distributed Common Ground System to the future joint force. As we begin to draw away from the environments of recent wars there is great need to reflect on what happened so we can improve our future efforts. Dealing with establishing and sustaining the rule of law where it has been lost is certainly an important area to review as Patrick Reinert and John Hussey lay out what needs to be done in places our joint force might go.

In keeping with the Civil War theme of my opening thoughts on leadership, John Erath presents his essay on that period and what he sees as lessons for strategic leaders today. We also have three excellent book reviews that will lead you to some important works for your professional reading. This edition finishes with an important essay on the future of joint operations and planning doctrine and the Joint Staff's update on joint doctrine development status.

We note with sadness the passing of the Honorable James P. Terry, whose distinguished career included 27 years of service in the Marine Corps, beginning as an infantry officer and finishing as a colonel, as well as serving as the legal counsel to Chairman of the Joint Chiefs of Staff General Colin Powell, holding senior positions in the State and Interior Departments, and finally serving as Chairman of the Board of Veterans' Appeals at the Department of Veterans Affairs. Jim was a frequent contributor of both articles and book reviews to *JFQ* and was a great person to talk with, as all the editors of this journal knew that special pleasure. Jim was a great supporter of many causes with jointness and joint education among the most important to him. Semper Fi, Jim.

If I were allowed to add one leadership attribute to those the Chairman has set out that President Lincoln cultivated throughout his entire life, it would be the willingness and drive to read, learn, write, and speak out on the issues of the day that were important to him. We look forward to receiving your efforts to speak out on the issues that matter to you in support of the future joint force and our nation. **JFQ**

William T. Eliason
Editor in Chief

Secretary of Homeland Security Jeh Johnson hosts President Obama at National Cybersecurity and Communications Integration Center (DHS/Barry Bahler)

Rethinking the Cyber Domain and Deterrence

By Dorothy E. Denning

As the Department of Defense (DOD) formulates strategy and doctrine for operating in cyberspace, it is vital to understand the domain and how it relates to the traditional domains of land, sea, air, and space. While cyberspace has distinct technologies and methods, it shares many characteristics with the traditional domains, and some of the conventional wisdom about how cyberspace differs from them does not hold up under examination.

These similarities are especially relevant when it comes to strategies for deterrence. Just as any attempt to develop a single deterrence strategy for all undesirable activity across the traditional domains would be fraught with difficulty, so too for cyberspace. Yet this is how many authors have approached the topic of deterrence in cyberspace. Instead, by focusing on particular cyber weapons that are amenable to deterrence or drawing

Dorothy E. Denning is a Distinguished Professor in the Department of Defense Analysis, Graduate School of Operational and Information Sciences, at the Naval Postgraduate School. The author thanks John Arquilla, Peter J. Denning, and Kalev Sepp for helpful comments on an earlier version of this paper.

from existing deterrence regimes, the issues become more tractable.

But first, two key attributes of cyberspace must be examined, as they show why cyberspace strongly resembles traditional domains. These are the roles played by man vs. nature and the malleability of the domains. Other similarities across the domains are described later in the context of deterrence.

Man and Nature

Conventional wisdom holds that cyberspace is made by man, whereas the traditional domains were created by nature. This is reflected in the *Department of Defense Strategy for Operating in Cyberspace*: "Although it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space."[1] General Michael Hayden, USAF (Ret.), former Director of the National Security Agency and the Central Intelligence Agency (CIA), similarly noted: "the other domains are natural, created by God, and this one is the creation of man."[2]

This distinction of manmade vs. natural permeates the cyber warfare literature. Martin Libicki, a senior management scientist at the RAND Corporation and one of the leading thinkers about cyber warfare, writes, "Everyone concedes that cyberspace is man-made. This is what makes it different from its predecessors."[3]

While it is certainly true that cyberspace would not exist without the computers and networks created by man, all domains of warfare, with the possible exception of land, are fundamentally manmade. The maritime domain would not exist without boats, the air domain without planes, and the space domain without rockets and satellites. Indeed, these domains, along with their respective military forces, were created only *after* the introduction of naval vessels, military aircraft, and spacecraft, respectively. Even the domain of land is substantially manmade. Although land forces could in principle fight it out with sticks and stones, and move only on foot or the backs of horses and camels, they instead deploy a plethora of manmade tools, vehicles, and weapons to support operations over terrain that has been substantially altered by man through the construction of roads, bridges, tunnels, buildings, canals, pipelines, and so on. Indeed, urban warfare takes place in an environment that is predominantly manmade. Nature, and especially geography, still matter, but none of the traditional domains, including land, can be understood, let alone operationalized, in today's world without accounting for the artifacts of mankind and the changes man has made to the environment.

At the same time, cyberspace has a substantial natural component. It relies heavily on electromagnetic waves, as well as natural elements such as silicon. Indeed, the electromagnetic spectrum—that is, the range of all possible wavelengths and their associated frequencies, to include radio, infrared, and light waves—is crucial to communications in cyberspace. All communications, regardless of whether they are transmitted through the air or over wires or optical fibers, take the form of electromagnetic waves. And even though these waves are generated by manmade devices that convert digital information into continuously varying wave forms, they have the same physical makeup and are constrained by the same laws of physics as the naturally occurring ones in background radiation. Electromagnetic waves are to cyberspace much as land, water, air, and space are to the traditional domains of warfare. They are a medium for movement, in this case digital objects instead of people and equipment. The waves themselves travel through land, water, air, or space, so in a sense they are a medium within the other media—but then so too are rivers and canals with respect to land.

Computer networks, of course, are manmade. But they are like the manmade road and rail networks in the domain of land; both provide infrastructure over which much movement takes place. Moreover, just as the placement of roads and train tracks is strongly influenced by geography, so too is the placement of cyber infrastructure such as cell towers and cables.

There is another, perhaps even more fundamental reason why the man vs. nature dichotomy breaks down: all of the domains encompass more than just their physical manifestations. They are domains of human practice and, as such, constrained by the actions and decisions of humans. For example, even though the borders separating one country from another often follow natural geographic formations such as mountain ranges and bodies of water, they are set by man, as are the boundaries that separate one property owner from another within a country. Moreover, the legitimacy of these borders relies on human agreements, which in turn are backed by manmade laws, regulations, and means of enforcement. International borders are often at the root of conflict, such as those involving Ukraine, Georgia, Kashmir, and islands in the South China Sea. But even when borders are not in dispute, conflict can emerge over other human agreements, especially those of national governance. The civil war in Syria and recent coup in Thailand illustrate this fact.

Recognizing the role of humans in all domains of warfare is essential to understanding deterrence. Deterrence is fundamentally about influencing the decisions and actions (or inactions) taken by human beings, not nature. It is highly dependent on human agreements, both nationally and internationally.

At the international level, the Charter of the United Nations (UN) together with other international agreements, including the Geneva and Hague conventions and customary international law, form a body of agreements referred to as the Law of Armed Conflict (LOAC), which is concerned with state activity across all domains of warfare, prescribing conditions under which states may and may not use their military forces. State activity is also constrained by numerous other agreements that cover such areas as trade, travel, telecommunications, finance, the environment, energy, weapons, crime, and embassies.

At the national level, domestic laws, regulations, contracts, and other types of agreements, together with various means of enforcement including police and the

NASA's Mid-Infrared Instrument has camera and spectrograph that see light in mid-infrared region of electromagnetic spectrum (NASA/Chris Gunn/Rob Gutro)

criminal justice system, restrict activity within a state's borders. Within organizations, policies, procedures, and personnel agreements restrict the actions of their employees.

As domains of human practice, all domains of warfare are further constrained by the skill and initiative of their human practitioners, and by the resources those practitioners are able to acquire to meet their objectives. Nature, by itself, will not engage a foreign adversary. Militaries must plan, resource, and execute their operations, whether in cyberspace or a traditional domain of warfare. While some of the skills needed to operate effectively in the cyber domain differ from those in other domains of warfare, other skills such as the ability to communicate effectively, work with others, build trust, and manage projects do not.

It is tempting to think that it is easier, cheaper, and faster to act in cyberspace than in traditional domains. After all, it is just a matter of moving, processing, and storing bits—not people and physical objects. But resources and skillsets matter as much in cyberspace as any other domain. Lacking adequate bandwidth, for example, it may be faster to move digital objects by downloading them to portable media and shipping the media than by sending them over a slow network. And surely one of the reasons why terrorists still prefer bombs to bytes is that it is easier for them to build and deploy explosives than to achieve comparable effects with cyber weapons. Developing a sophisticated cyber warfare capability requires considerable upfront investment.

Malleability

The manmade vs. nature distinction has led to a conclusion that cyberspace is easier to change than the traditional domains. General Hayden, for example, wrote, "Man can actually change this geography, and *anything* that happens there actually creates a change in someone's *physical* space."[4] Libicki emphasized the importance of this aspect: "What matters is that cyberspace is highly malleable by its owners, hence its defenders, in ways other media are not."[5] If true, this would suggest that cyberspace might be more amenable to deterrence by denial, that is, through security defenses, than other domains of warfare.

While some things are easy to change in cyberspace, the overall malleability of the domain is severely limited by standards, interoperability requirements, legacy software, regulations, and the resources and inertia needed to make changes. The switch from version 4 to version 6 of the Internet Protocol (IP), for example, has been taking years. As of May 2014, the bulk of Internet traffic is still carried in version 4 packets, including over 96 percent of the traffic connecting to Google servers.[6] There are

many reasons for the slow adoption, but a survey of industry professionals found that the top reasons were transition costs, compatibility issues, and security concerns.[7] The security issues are interesting; while version 6 mandates support for encryption and authentication, it effectively breaks security products such as firewalls and intrusion prevention systems that were developed for version 4.

There are numerous other examples demonstrating the slow adoption of new Internet protocols and standards, including ones that would thwart many of the cyber attacks that plague cyberspace today, such as denial-of-service and phishing attacks that rely on spoofing an IP address, email account, or organization in cyberspace.[8] In addition, organizations can be slow to adopt improved versions of operating systems and application software, as illustrated by the many installations still running Windows XP and applications built for it, and they can be slow to install security patches for published vulnerabilities.

This lag in adoption is seen in industrial control systems that operate critical infrastructure such as power generation and distribution, oil and gas distribution, and water treatment and distribution. Many of these systems run legacy software that offers practically no security, but meets performance, reliability, and safety objectives that drove decisions before the threat of cyber attacks became an issue. To make matters worse, these systems are often connected to the Internet, exposing them to cyber threats for which they lack defenses. Operators may be reluctant to update and patch these systems for fear of breaking something and disrupting essential services.

Within the Federal Government, the ability to acquire new cyber technologies is hampered by procurement regulations. Acquisition delays of 5 to 10 years are not uncommon in the military.

The malleability of cyberspace is also constrained by the time and resources required to install infrastructure such as cables and satellites, as well as by the laws of nature. Fred Cohen, for example, showed three decades ago that it was impossible to develop a computer program that would detect any computer virus by either its appearance or its behavior.[9]

At the same time, traditional domains of warfare, especially land, can be reasonably malleable. While building highways and bridges can take considerable time, and mountains and forests are immovable, it can be relatively easy to make certain types of changes in some geographic areas—for example, to install surveillance equipment, plant and detonate explosives, and reposition troops—all of which can significantly impact military operations. In all domains, militaries have to contend with change and uncertainty brought on by adversary actions and nature.

Cyberspace itself is also increasing the malleability of other domains of warfare. With additive manufacturing, also known as three-dimensional (3D) printing, it becomes possible to transform digital blueprints into physical weapons and other types of devices. Instead of building a device in a manufacturing plant in one country and then shipping it to a facility in another, a digital blueprint can be transmitted to a 3D printer at the intended destination.

Cyberspace has an advantage over the traditional domains in that if a cyber operation alters digital objects without affecting objects external to cyberspace, its effects can be undone by restoring the original bits. Thus, if a cyber operation shuts down a power generator by tampering with bits in its control system, for example, it may be possible to restore power simply by resetting the bits. By contrast, if the generator is shut down with a bomb, it must be physically rebuilt or replaced. Additive manufacturing, however, may someday remove even some of this advantage.

Deterrence in Cyberspace

The literature on cyber deterrence reveals many challenges to the very concept.[10] These include the:

- difficulty of attributing cyber attacks to their perpetrators
- ease of acquiring cyber weapons and conducting cyber attacks
- broad scope of state and nonstate actors who engage in cyber attacks for a multitude of reasons and against both state and nonstate targets
- short shelf life of many cyber weapons
- difficulty of establishing thresholds and red lines for cyber aggression
- difficulty of setting and enforcing international norms regarding cyber behavior
- challenges associated with avoiding escalation.

Authors who have compared cyber deterrence with nuclear deterrence have generally found that the principles that have made nuclear deterrence effective for over half a century fall apart in cyberspace.[11]

One reason why the concept of cyber deterrence raises so many challenges is that the term is extremely broad. In no other domain of warfare do we address the topic of deterrence across an entire domain. There is no notion of "land deterrence," "sea deterrence," "air deterrence," or "space deterrence." Rather, we direct our attention to particular weapons and activity. Some of these may be tied to specific domains of warfare and even geographic areas, such as deterrence of Somali pirates in the Gulf of Aden, but others are not, such as deterrence of state-level aggression generally.

Consider nuclear deterrence. It is about a specific type of weapon, not a domain of warfare. In fact, it crosses all domains of warfare, as nuclear weapons can be launched from land-based missiles, fired from submarines, or dropped from bombers against targets in any domain. The success of nuclear deterrence is contingent on the nature of the weapon, which inherently limits its casual development and deployment. Nuclear deterrence is directed primarily at nation-states and, by extension, state-sponsored terrorists. It relies primarily on retaliation or punishment, including nuclear counterstrikes leading to mutually assured destruction. But nuclear deterrence also depends on restricting the states that have nuclear

arsenals and the spread of the knowledge and materials required to develop the weapons, sometimes called "deterrence by denial." This in turn is supported by the establishment of international norms and agreements that limit the acquisition and use of nuclear technologies, such as the Nuclear Non-Proliferation Treaty of 1968. Both denial and norms can have a deterrent effect by dissuading parties from even attempting to acquire nuclear weapons.

In traditional domains of warfare, there are all sorts of nefarious activity that one would like to deter, including bombings, chemical and biological attacks, genocide, terrorism, armed invasions by foreign military forces, theft, bribery, fraud, extortion, embezzlement, insider trading, political corruption, arson, murder, espionage, vandalism, kidnapping, sexual assault, child and elder abuse, and animal abuse. Some of this activity falls in the area of national security and military operations, but other activity falls in the area of domestic crime and law enforcement. Given the enormous scope of the actors and activities involved, it would be difficult to develop an effective deterrence strategy that covered it all. Attempting to do so would inevitably raise many of the same problems that have surfaced in studies of cyber deterrence. For example, like many cyber weapons, many physical weapons, to include knives and guns, are easy to acquire and difficult to control. Street crimes such as vandalism, arson, and theft can be easy to commit but difficult to prevent and attribute.

Cyberspace is becoming as rich a domain of activity as land. It supports a large and ever growing set of operations relating to communication, finance, business, commerce, education and training, research, entertainment, health care, the environment, energy, government, military operations, and more. And, like all domains of warfare, it is used for both civilian and military activity. To get our hands around deterrence in cyberspace, we need to move beyond general statements about the domain as a whole to statements about situations where deterrence could play a meaningful role. One might argue that cyber deterrence is really about a particular type of weapon and not the domain, and in that regard its focus is similar to nuclear deterrence. But the comparison is not fair. Cyber weapons constitute the entire set of methods and tools that can produce effects in cyberspace, ranging from simple weapons that are readily acquired and used by "script kiddies" with no real skill in the domain, to those that require an advanced capability to develop and successfully deploy, such as was the case with Stuxnet. They also range from weapons whose effects are minor to ones that could potentially lead to death. By contrast, nuclear weapons are a highly lethal subset of all explosives, and explosives in turn are just a subset of all the physical weapons that can produce effects in traditional domains.

Just as we do not sweep all physical weapons into a single strategy of deterrence, we should not try to sweep all cyber weapons into a single strategy. Rather, we need to narrow our treatment of deterrence as it relates to cyberspace. The following suggests two approaches: one centered on particular cyber weapons, the other on existing deterrence regimes. These are not exclusive, but rather orthogonal or complementary. Others have advocated tackling the deterrence issues by taking into account the geopolitical context[12] and applying principles of tailored deterrence, both of which can be used with the ones suggested in this article.[13]

Deterrence for Classes of Cyber Weapons

The first approach is to focus on relatively narrow classes of cyber weapons where deterrence might be feasible. For example, consider nuclear electromagnetic pulse weapons, sometimes referred to as nuclear EMPs or simply NEMPs. These are nuclear weapons that would be detonated at high altitudes above Earth with the objective of damaging electronic devices rather than killing persons or blowing up buildings. Because so much critical infrastructure depends on computers and other electronic devices, the effects of a well-placed NEMP attack could be devastating not only to cyberspace but also to all domains of activity and society as a whole. Testifying before Congress, former CIA Director James Woolsey noted that a nuclear warhead, launched with a medium-range missile from the Gulf of Mexico and detonating at an altitude of 400 kilometers, would generate an EMP field on the ground with a radius of 2,200 kilometers, "covering all of the contiguous 48 United States, causing a nationwide blackout and collapse of the critical infrastructures everywhere."[14]

Because NEMPs are nuclear weapons, they automatically fall under the umbrella of nuclear deterrence. In addition, unlike nuclear weapons that detonate directly against their targets, their effects can be denied, as electronics can be hardened against the damaging radiation emitted by these weapons. While such hardening may not be practical for all electronic devices, it might be worth applying to critical infrastructures vital to society.

Numerous cyber weapons lend themselves to deterrence by denial, including any weapon that can be thwarted with the adoption of existing security technologies and practices. As noted earlier, many denial-of-service and phishing attacks can be stopped with anti-spoofing technologies that already exist. Deterrence strategy could focus on stimulating greater adoption of these technologies and on developing additional ones. In addition, many cyber weapons exploit vulnerabilities in existing systems for which there are patches or fixes. Deterrence strategy could promote more rapid and widespread adoption of these fixes. Strong defenses can convince would-be perpetrators that a cyber attack will likely fail and, therefore, is not worth implementing.

Some classes of cyber weapons might be suitable for deterrence by punishment. Even though many cyber attacks are difficult to attribute and therefore punish, others are not. Cyber activists operating under the banner of Anonymous, for example, used a cyber weapon called the Low Orbit Ion Cannon to conduct denial-of-service attacks against targeted Web sites. This tool did not, however, give its

Shelby Cobra—approximately 1,400-pound vehicle containing 500 pounds of printed parts made of 20 percent carbon fiber—produced by Big Area Additive Manufacturing Machine, which manufactures strong, lightweight composite parts in sizes greater than 1 cubic meter (DOE)

users anonymity, and 19 people who used it during "Operation Payback" in 2011 against PayPal, Mastercard, and Visa were identified and arrested, including 14 in the United States.[15]

Still other types of cyber weapons might be suitable for deterrence by norms and agreements. NEMPs, as nuclear weapons, fall in this category. If a cyber weapon is ever developed that could cause massive deaths, it might be similarly categorized.

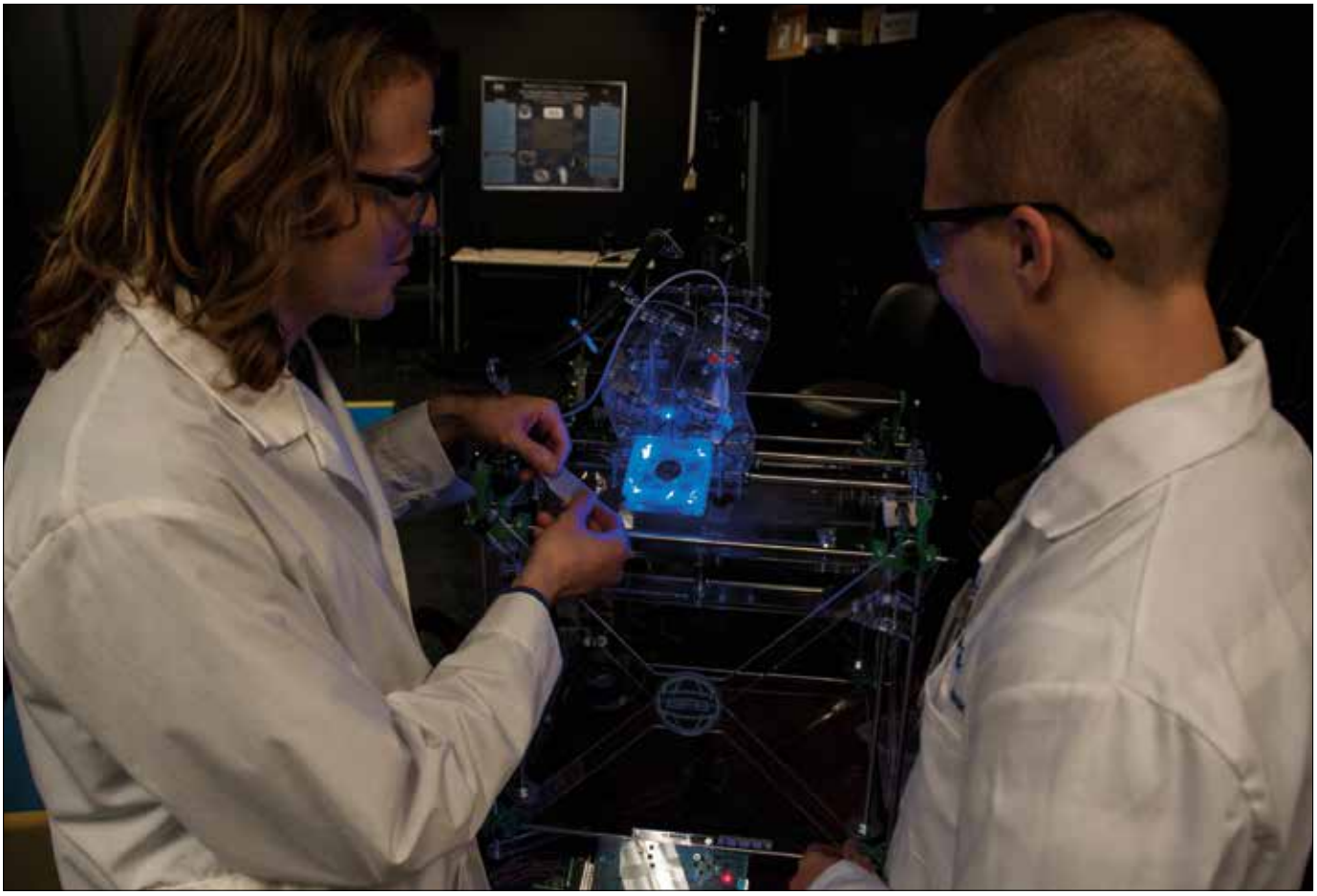
Deterrence Through Established Regimes

A second approach to deterrence in cyberspace is through the application of deterrence regimes established for other kinds of activity. As already noted, we can do this with NEMPs, drawing on existing strategies and mechanisms for nuclear deterrence. But we can also do it more broadly and apply established strategy for deterring state-level aggression and crime by nonstate actors.

LOAC is particularly relevant to deterring state-level aggression. Although it predates cyberspace, government officials, scholars in the area of international law, and cyber experts generally agree that it applies to cyberspace. A UN group of government experts affirmed this: "International law, and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible" cyberspace.[16] The Tallinn Manual, sponsored by the North Atlantic Treaty Organization, offers rules for applying LOAC to cyberspace,[17] and DOD has stated that its actions in cyberspace will be governed by LOAC and all other applicable domestic and international legal frameworks.[18] LOAC supports deterrence by both norms and punishment by establishing principles for the use of force by states and for responses by the international community to state acts of aggression.

In addition to LOAC, other international agreements might serve to deter certain activity. One such agreement is the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights, which requires participating nations to protect trade secrets. Both the United States and China are members of WTO, and in response to the indictments of five members of China's People's Liberation Army for stealing trade secrets, Senator Charles Schumer called on the U.S. representative to the WTO to file suit at the WTO against China for state-backed cyber espionage.[19]

Well-tempered statecraft can deter aggressive state behavior in all domains of warfare. Also, to the extent that the affairs of states are intertwined, especially



Research engineers use 3-D printer in their work at FDA (FDA/Michael J. Ermarth)

economically, there is some deterrence by interdependency or entanglement; if one state harms another, it will also harm itself.

Crimes committed by nonstate actors have been deterred traditionally through norms via religious and moral teachings as well as crime statutes; by punishment via law enforcement and the criminal justice system; and by denial via fences, locks, alarms, guards, and other mechanisms that control entry into protected spaces. In addition, surveillance devices such as security cameras can help catch criminals such as shoplifters, muggers, and vandals who would otherwise not be identified and caught, thereby strengthening deterrence by punishment. Community policing, especially in "hot spots," and neighborhood watch groups can also deter street crime.

Cyber crimes can be deterred by the same types of mechanisms. In the United States, the Computer Fraud and Abuse Act of 1986, together with its amendments and other laws that apply to cyberspace, set norms for acceptable behavior in cyberspace. Many of these norms appear in the domestic crime laws of other countries as well. In addition, they are included in the Council of Europe (COE) Convention on Cybercrime. As of March 2014, 42 countries had ratified the Convention and 11 more had signed it, showing strong international consensus regarding much cyber activity.[20] While these laws obviously have not deterred those persons who commit cyber crimes, they likely deter those who view themselves as law-abiding citizens.

At least one study has shown that deterrence by punishment applies to cyber crime. Researchers at the National University of Singapore found a 36 percent reduction in cyber attacks relating to 49 reports of government enforcement actions in eight countries.[21] However, more studies are needed to validate (or refute) these results and to determine factors that can make a difference. While it would be overly optimistic to assume that the persons behind all cyber attacks could be caught and punished, improved methods of cyber forensics and attribution, coupled with greater international cooperation such as that facilitated by the COE Convention on Cybercrime, could lead to greater deterrence by punishment.

Deterrence by denial is practiced every day in cyberspace via cyber security mechanisms and practices, including the regular installation of security patches, the use of strong methods for authentication, and the application of firewalls, black and white lists, intrusion prevention systems, antivirus tools, encryption, and so forth. We can aim for even more effective cyber security in the future by placing greater emphasis on security during the design, development, installation, and operation of new cyber technologies, but it is not likely to ever be completely foolproof, for

much the same reason that crime overall will never be fully eliminated. Still, denial offers the best means of deterrence, whether in cyberspace or not, in those situations where it can be applied and is cost effective. Much of the literature on deterrence in cyberspace recognizes this.

Conclusions

Cyber technologies are inherently different from those that define the traditional domains of warfare. After all, they are used to move, process, and store digital objects across computer networks—not people and physical objects across land, sea, air, and space. But technology aside, cyberspace shares many of the same characteristics as other domains of warfare. All have both manmade and natural elements, and the malleability of all is subject to considerable constraint. Importantly, all are domains of human practice, characterized by a wide range of activity by both state and nonstate actors, some of which is hard to attribute, and by a variety of weapons ranging in availability, cost, and effects produced.

Because cyberspace is such a rich domain, studies of "cyber deterrence" raise as many problems as would be raised by a comparable study of "land deterrence." This does not mean that deterrence in cyberspace is impossible, only that a more focused approach is needed, as has been followed in traditional domains of warfare. One possible approach is to consider classes of cyber weapons that lend themselves to deterrence. Another is to consider existing deterrence regimes, including international regimes governing nation-states and domestic regimes governing nonstate criminal behavior. These approaches can be combined with others that are tailored to particular actors or geopolitical contexts. Together, they may offer a tractable approach to deterrence in cyberspace. **JFQ**

Notes

[1] *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 5, available at <www.defense.gov/news/d20110714cyber.pdf>.

[2] Michael V. Hayden, "The Future of Things 'Cyber,'" *Strategic Studies Quarterly* (Spring 2011), 4, available at <www.au.af.mil/au/ssq/2011/spring/hayden.pdf>.

[3] Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012), 324, available at <http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf>.

[4] Hayden, 4.

[5] Libicki, 324.

[6] IPv6 Statistics, accessed May 14, 2014, at <www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption>.

[7] Aman Yadav et al., "IPv6 Protocol Adoption in the U.S.: Why Is It So Slow?" Capstone paper, University of Colorado, May 4, 2012, available at <http://morse.colorado.edu/~tlen5710/12s/IPv6Protocol.pdf>.

[8] Examples of protocols and standards that would significantly improve cyber security include the Network Ingress Filtering standard, which would put an end to many large-scale denial-of-service attacks that rely on Internet Protocol address spoofing; the Domain Name System Security Extensions, which protect against cyber attacks such as domain spoofing and hijacking; the Secure Border Gateway Protocol (BGP), which addresses serious security issues with BGP that can lead to network blackouts and make traffic more vulnerable to adversary eavesdropping; and Domain-Based Message Authentication, Reporting and Conformance for authenticating email, which would combat many email security issues such as phishing and spam that rely on spoofing the sender.

[9] Fred Cohen, "Computer Viruses: Theory and Experiments," University of Southern California, August 31, 1984, available at <http://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html>.

[10] See, for example, Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009); Martin C. Libicki, "Deterrence in Cyberspace," *High Frontier* 5, no. 3 (May 2009), 15–20; "Letter Report for the Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy," Washington, DC, National Research Council, March 25, 2010; Jonathan Solomon, "Cyberdeterrence Between Nation-States: Plausible Strategy or a Pipe Dream?" *Strategic Studies Quarterly* 5, no. 1 (Spring 2011); and Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security* 7, no. 1 (2013), 54–67.

[11] See, for example, David Elliott, "Deterring Strategic Cyberattack," *IEEE Security & Privacy* (September/October 2011), 36–39.

[12] Will Goodman, "Cyber Deterrence: Tougher in Theory Than in Practice," *Strategic Studies Quarterly* (Fall 2010), 102–135.

[13] Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), 309–340.

[14] James R. Woolsey, "Testimony Before the House Committee on Energy and Commerce," Washington, DC, May 21, 2013, available at <http://highfrontier.org/r-james-woolsey-testimony-before-the-house-committee-on-energy-and-commerce-may-21-2013/#sthash.PsBE9is7.dpbs>.

[15] Frazier McGinn, "Anonymous Arrested for DDoS Against PayPal," *Examiner.com*, July 19, 2011, available at <www.examiner.com/article/anonymous-arrested-for-ddos-agaisnt-paypal>.

[16] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Report A/68/69 (New York: United Nations General Assembly, June 24, 2013).

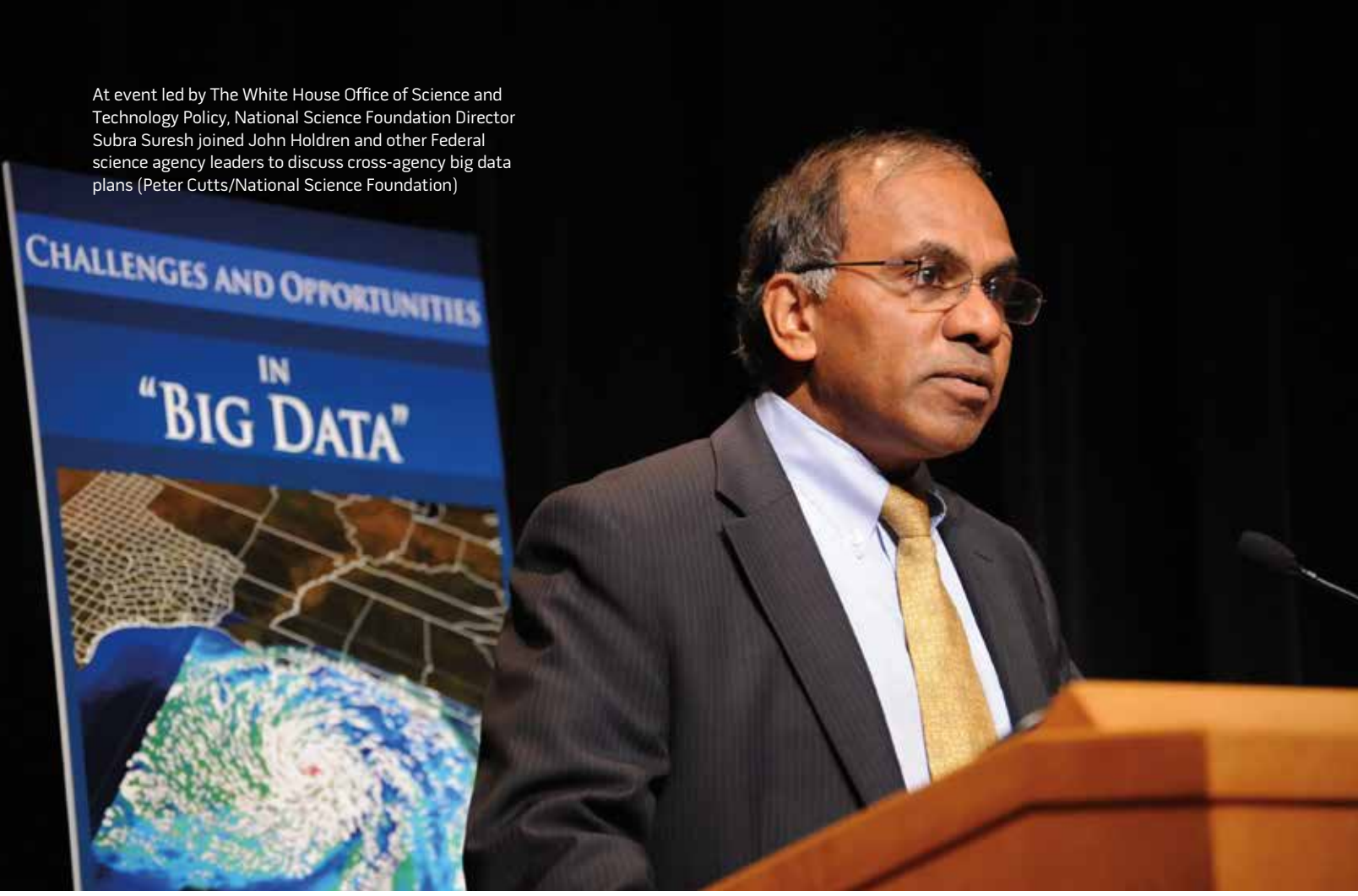
[17] Michael Schmitt, ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

[18] *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* (Washington, DC: Department of Defense, November 2011).

[19] Press release from the office of Senator Charles E. Schumer, United States Senator for New York, May 22, 2014.

[20] Council of Europe, "Convention on Cybercrime," available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG>.

[21] I.P.L Png and Chen-yu Wang, "The Deterrent Effect of Enforcement Against Computer Hackers: Cross-Country Evidence," Workshop on the Economics of Information Security, March 2007, available at <http://weis2007.econinfosec.org/papers/77.pdf>.



At event led by The White House Office of Science and Technology Policy, National Science Foundation Director Subra Suresh joined John Holdren and other Federal science agency leaders to discuss cross-agency big data plans (Peter Cutts/National Science Foundation)

Framing the Big Data Ethics Debate for the Military

By Karl F. Schneider, David S. Lyle, and Francis X. Murphy

Big data is everywhere these days. It shows up in many realms of contemporary life, ranging from how people are guided to potential purchases as they shop online, to how political campaigns win elections, and even to when farmers plant crops and apply fertilizer to their fields.

While there is no denying the value that comes from data integration and information availability made possible by modern computing power, there are many associated challenges that relate to the privacy of the individual, security of personal data, and reach of decisions influenced by big data. These concerns describe an emerging discipline known as the ethics of big data. This growing conversation is relevant for the military, given both the potential gains from big data collection and analysis as well as the simple fact that big data is here to stay.

In this article, we first define what is actually meant by the terms *big data* and *ethics of big data*, explore the challenges associated with big data, discuss some examples and implications for the military, and conclude with a framework for addressing many of these challenges.

Karl F. Schneider, SES, JD, LL.M., is Principal Deputy Assistant Secretary of the Army for Manpower and Reserve Affairs. Lieutenant Colonel David S. Lyle, USA, Ph.D., is Director of the Office of Economic and Manpower Analysis in the Department of Social Sciences at the United States Military Academy at West Point. Major Francis X. Murphy, USA, is a Research Analyst in the Office of Economic and Manpower Analysis.

The term *big data* or *mega-data* refers to a collection of data sets so large and complex that the data become difficult to process using on-hand database management tools or traditional data processing applications. Big data arises from follow-on analysis of existing large data sets and the capture of software logs and information-sensing mobile devices such as cameras and global positioning systems. E-commerce retailers such as Amazon can exploit data on past Internet browsing histories to deliver targeted, personalized advertising to specific customers. As new technologies emerge and become more affordable to collect, process, and store data, the volume of data collection grows exponentially; some 2.5 x 1018 exabytes of new data are created every day.[1] In addition to the sheer volume of information in big data, these data collection efforts increase the breadth of information available to analysts while compressing the delay between data collection and its subsequent analysis. For example, researchers at the University of Michigan now construct social media indexes of labor market activity such as job loss and job posting using text searches of Twitter posts, a tool that is much more accurate in predicting hiring trends than the consensus forecasts of experts and that is close to being available in real time.

A fairly new and emerging field, the ethics of big data has started to address some of the challenges associated with big data, many of which are of an "ought to" rather than an "is" nature. Big data itself is ethically neutral; it is the actual *use* of big data that raises ethical questions. Thus, the ethics of big data concerns more than simply the matter of morality. Rather, it includes issues such as the privacy, validity, security, transfer, and analysis of big data as well as the business decisions or policy implementation that follow from big data insights. These topics have far-reaching consequences when the data relate to sensitive homeland security matters, individual medical records, or more broadly to data containing personally identifiable information, which often include sensitive information such as name, date of birth, and Social Security Number (SSN).

Understanding Big Data and the Ethics of Big Data

An important starting point for understanding big data is to consider the structure of the underlying information. Big data is referred to as structured when it is in traditional rows and columns such as one would find in a standard spreadsheet. At the other end of the continuum, photographs or feeds are considered unstructured data. Free-form text in a social media status update is an example of semistructured data and sits at the middle of this continuum because it has features similar to both structured and unstructured data.

One of the most appealing aspects of big data and its applications is the ability to study a larger share or sample of an underlying population. Large samples allow researchers, policymakers, and business analysts to better approximate how behavioral responses vary across different segments of an entire population. They also allow for increased understanding of heterogeneity, or granular differences across variables within data. For example, in figure 1, we compare two samples of different size drawn from the same underlying population. Having access to a larger sample with more granular, accurate, and timely data—such as in Sample B—allows for a more complete analysis of behavior among those in the underlying population.

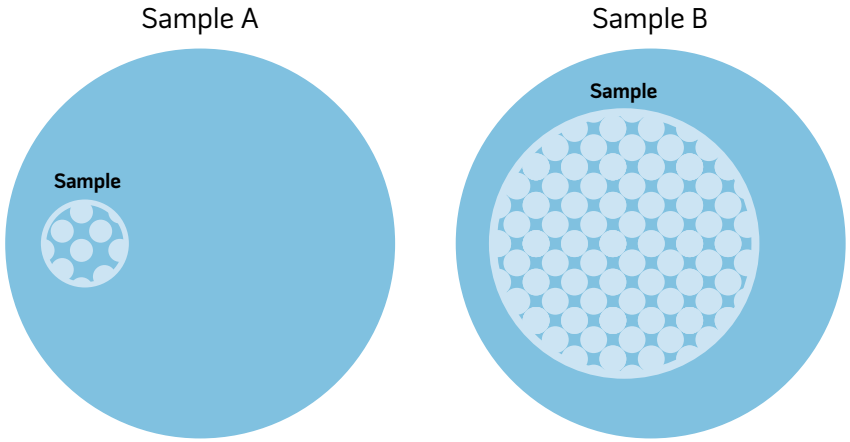
There is a growing dialogue aimed at formalizing norms related to the ethics of big data. The White House and Massachusetts Institute of Technology recently cohosted a forum titled "Big Data Privacy: Advancing the State of the Art in Technology and Privacy." In April 2014, the University of Virginia hosted the first "National Conference on Big Data Ethics, Law and Policy." The Council for Big Data, Ethics, and Society also convened in 2014 to address security, privacy, equality, and access to big data. Standards related to the collection and use of big data are the focus of an emerging field of study; in *Ethics of Big Data: Balancing Risk and Innovation*, Kord Davis advocates for a framework based on identity, privacy, ownership, and reputation.[2] He believes that asking questions along these dimensions will help to establish common ground for discussing the ethics of big data. Similar to the work by Davis, a law review article by Neil Richards and Jonathan King suggests that principles of privacy, confidentiality, transparency, and maintaining identity should govern data flows and inform the establishment of big data norms.[3] Finally, the White House recently released a major study on big data that emphasizes, among other things, the need to preserve personal privacy even as the promise of big data suggests better delivery of nearly every type of public good.[4]

These early efforts to address the ethics of big data have helped elevate the importance of this topic and have highlighted the need for a common language and clear guidelines that promote understanding of expectations and best ethical practices. Implicit within the area of big data ethics is an application of common practices to each specific institution. For example, the issue of trust may have greater weight for an organization such as the military than for an organization such as Facebook. This is not to suggest that trust is not important in the private sector (because it certainly is); however, trust does have an amplified importance in the military because life and death outcomes as well as national security are at stake.

Benefits of Big Data

As discussed, big data has many practical uses in fields such as research, disease prevention, and business analytics. Examples of big data include Google Analytics on the frequency of Internet searches to predict share price movements of publicly traded companies and the Sloan Digital Sky Survey, which collects 200 gigabytes of astronomy-related data per night. eBay and Facebook also maintain almost unfathomable quantities of data on consumer transactions and user-uploaded photos, respectively. Big data collection of consumers' Internet browsing and purchasing histories helps e-commerce firms such as Amazon build algorithms for applications such as its "You Might Like" feature. The retailer here relies on big data to recommend products

Figure 1. Big Data's Impact on Sample Sizes



that the Internet shopper is likely to purchase.

Big data is also relevant to decision-makers in fields as diverse as agriculture and political campaigns. Big data analysis of variation in soil fertility and nutrient needs within a field—coupled with global positioning technology—now allows farmers to customize the application of fertilizers, reducing input costs while increasing yields. Since 2004, political campaigns have used big data for "micro-targeting"—personalizing campaign-messaging based on voter demographics. Campaign strategists increasingly use big data to identify the most efficient uses of campaign funds to persuade prospective voters to go to the polls and vote for their candidate.

An example of big data's potential benefit to the military is the ongoing empirical research measuring the impacts of military service on lifetime earnings. This project requires the development of a unique data set containing individual-level structured data on millions of veterans across nearly two decades. Through a series of data merges, administrative data are joined with information on veterans' disability compensation, GI Bill usage, as well as unemployment benefits receipt and annual earnings.

Big data allows the researcher to combine and subsequently analyze all of the above dimensions of a veteran's experience. Thorough analysis of this data by skilled researchers can identify the long-term impacts of military service and the use of specific military benefits. While the data effort is immense, the proposed research outcome is critical to society and its understanding of the costs and benefits of the all-volunteer force. This is just one research-driven example of the power and utility of big data when it is harnessed properly.

Although the above example illustrates the potential value of big data to the military, it also highlights the larger ethical implications of assembling big data. First, the collection and use of big data cannot compromise the organization's core value of trust: that the military will both provide for the national defense and also look out for the best interest of its Servicemembers. The military must recognize that the individual has enduring rights related to personal information, regardless of whether a third party or agency has access to or custody of that data.[5] Second, as we address in more detail later, it is crucial to realize that big data itself is not a cure-all as some have suggested. Rather, big data is complementary to existing methods as a high-powered analytical tool that nonetheless requires the context of understanding the problem, considering theory, formulating hypotheses, and testing for relationships.

Challenges of Big Data

While the opportunities presented by big data are immense, the associated challenges are important and must be considered by any person or organization involved in the collection and analysis of big data. Accordingly, we group challenges associated with big data into six principal areas:

- use and transfer of personally identifiable information (PII)
- merging and combining data sets
- policy formulation at the individual and group levels
- costs associated with use and analysis
- personnel challenges
- general analysis and interpretation.

The first challenge comes from the use and transfer of PII, which is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. The big three identifying variables are name, date of birth, and SSN. Together, these three pieces of information can almost always allow individuals to be identified within the data. There are some important distinctions concerning the nature of this information. PII can be sensitive or insensitive in terms of the consequences of its release or use. It can also be voluntarily or involuntarily collected from the subject, and the subject may be aware or unaware that the data have been collected or used. Finally, the data may be required by the military, as in the case of information on health conditions, or the data may be extraneous resulting from recent browsing history, for example. These distinctions will dictate, for instance, the level of security required for storing or transferring the data and whether the individual should be informed about potential uses of the data. It is also important to realize that these distinctions are dynamic and that the custodian of the data has to be constantly aware of the changing nature of data.

One of the key attributes of big data is that much of it follows from the integration or derivative analysis of data that already exists. The project on veterans' lifetime earnings is an example. Whenever big data is generated through the combination of existing data sets, there is the potential that previously anonymous data can become identifiable for an individual as a result of being merged with other

data. The new and larger data sets that result from combining data like this almost certainly rely on unique identifiers such as SSNs for accurate merging, and what results may have a new level of sensitivity. For instance, combining For Official Use Only (FOUO) information on the members of a military unit with FOUO information on unit locations in contingency operations will lead to a larger data set that is now classified as Sensitive. A related concern is the privacy right of the individual when a custodial entity is merging and sharing data. The purpose of the merge and the nature of the data dictate whether the subjects need to be aware of the merge or perhaps must even give permission before merging. Moreover, the riskiness of the data-sharing increases as it gets farther away from the source; merging Department of Defense (DOD) data with other DOD entities presents less risk than merging that same data with private corporations. Whether merging inside or outside of the military, deliberate care must be taken to mitigate the amount of information that merging entities gain. Many straightforward encoding techniques for merged data are available that can significantly reduce what is actually shared with the outside party.

Next, there are ethical implications concerning the use of big data analysis for policy at the individual or group level. Policymakers must be careful about how they use insights derived from big data, whether that data are unwillingly or willingly provided by the subject. Servicemembers have a right to privacy, and it can be problematic for an organization such as the military to use an individual's data against him.[6] For instance, imagine that the military conducts an analysis of Sergeant Smith's use of medical care benefits. If DOD enacted Service-wide policies based on that analysis, the ethical concerns are minimal. Suppose, instead, that one of the Services targeted Sergeant Smith with new premiums based on the data analysis. Given the unique mission and culture of the military, this example of micro-targeting would likely be viewed as a breach of trust and hence an inappropriate use of big data. In fact, such initiatives could engender resentment, lead to unintended changes in healthcare use, and even provide individuals with a strategic incentive to misreport their preferences for healthcare services as well as actual use.

Thus far, we have focused on the security challenges inherent in assembling big data within the military. Effective use of big data also requires *time*, *talent*, and *money*, all of which are scarce resources within any organization.

Identifying the necessary data and then constructing big data take significant effort and time. For example, the U.S. Army's personnel database has more than 2,000 variables per observation. However, a personnel analyst might routinely use only 200 or fewer of these. Extracting the relevant variables from this larger data set and then preparing them for analysis are time consuming and require individuals with both institutional knowledge of the Army and expertise in database management. Coordinating data merges with other government agencies is a lengthy process as well, and again requires individuals with expert knowledge. Moreover, collecting, storing, and safeguarding big data can require costly investment in state-of-the-art infrastructure and security software. The costs associated with training personnel to use big data, and subsequently providing sufficient tenure to these personnel so that the military can recoup the investments in developing this institution-specific knowledge, are substantial. In fact, this tenure problem may be one of the biggest challenges for the military, since the existing promotion system encourages frequent job-switching.

Big data reinforces the need for internal control mechanisms, such as institutional review boards (IRBs), which provide important oversight. However, the military has historically confused Privacy Act requirements and Human Subjects requirements with its IRBs. Human Subjects protections apply to some, but not all, information protected by the Privacy Act. Human Subjects protections are enforced by IRBs with the purpose of ensuring that a study is conducted ethically and without imposing any harm on an individual. These protections are designed to prevent abuses of human subjects in *experiments* and do not apply to policy analysis of existing administrative data. This is a key distinction that leadership must appreciate and support.

Similarly, big data implementation raises personnel challenges. The military must be deliberate in selecting and training personnel who use big data. Big data requires server and storage hardware, software, system administrators, database administrators, and analysts; each of these jobs requires specific skill sets. The development and continuous maintenance of those skills entail significant investments. DOD must also determine levels of access for anyone who interfaces with big data. Moreover, each class of military personnel (enlisted, officer, civilian, contractor) that works with big data not only provides unique benefits but also presents unique challenges and risks. Reiterating, extended tenure is a necessary condition for analysts using big data.

Finally, many challenges are related to the general analysis and interpretation of big data. There is an overriding temptation to equate the sheer quantity of the data with the mistaken assumption that any findings from such massive data must be meaningful. This belief is particularly dangerous since big data—based on sheer sample size—tends to produce many statistically significant findings, even if the proposed relationships are spurious and the analytical methods inappropriate. Regardless of the volume of data, analysis must be guided by relevant theory and sound statistical inference. In other words, big data must be paired with *big judgment* for the analysis to have practical policy applications or business decision relevance.[7] The often repeated mantra in the social sciences, "correlation does not imply causation," certainly rings true here. The popular economics writer Charlie Wheelan addresses this distinction in his 2013 book *Naked Statistics*, in which he imagines a study linking 5- to 10-minute outdoor breaks taken by office workers to increased rates of lung cancer. Of course, it is not the outdoor breaks that are causing cancer, but rather the smoking of cigarettes while outside on

Results of bacterial susceptibility tests were fed into computer and used to create printouts of data showing worldwide patterns of bacterial resistance to antibiotics (FDA)

the break that is the causal factor.[8] Thus, analysts must understand underlying sources of variation and consider inter-variable relationships so that they can differentiate between true causal relationships and mere correlations.

Illustrating the Challenges of Big Data

The Commander's Risk Reduction Dashboard (CRRD) is a current big data application in the Army that illustrates several of the big data challenges outlined above. The Army is increasingly integrating a variety of personnel data and relying on analysis of it to inform decisions at local command and higher levels. Launched in January 2014, the CRRD consolidates information from multiple sources—including medical records, deployment data, and correction actions—to provide unit commanders current snapshots of personnel who might be at high risk of manifesting suicidal behaviors. The CRRD takes the form of a software application that commanders access through Sharepoint, and it represents one effort the Army is using to address the recent increase in suicides among its ranks.

Much of the data in the application (and others that are similar) are personally identifiable and thus sensitive in nature, so there are immediate concerns about security, proper use, and general privacy and identity of individuals. Specific to the CRRD, there must be clear policies for access and transfer of that data: who needs to see the data outside of the command team and through what media? What happens when a Soldier transfers units? A related concern is whether the Dashboard program should apply algorithms to the data and make predictions, or simply allow the commander to observe and then process the raw data himself. Similarly, there is a chance that this exercise in statistical risk projection (whether done by the algorithm or the commander) could lead to prejudgments about a Soldier's performance and potential, particularly in the case of a Soldier trying to make a fresh start in a new unit. What if that Soldier misses out on a promotion, key assignment, award, or superior evaluation because the algorithm has determined that he is at risk for suicide-related behavior? Is this outcome fair? Does it violate the Soldier's right to privacy? Will uninformed use of this data actually increase the Soldier's risk of self-harm? Does the military's prerogative to prevent suicides—arguably at any cost—override these concerns about privacy and fairness? These and other questions capture many of the current dilemmas associated with the use of big data.

A Framework for Big Data in the Military

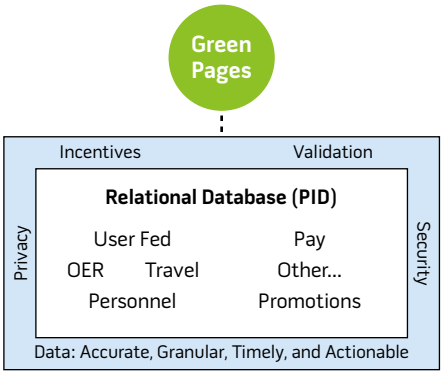
Given the challenges associated with big data and the striking relevance of those challenges to the Army in applications such as the Commander's Dashboard. In this framework, military big data is bound by pillars of privacy and security while incentives and validation result in data that are accurate, granular, timely, and actionable. Firewalls protect data so that authorized users can access, analyze, and use this data in a secure environment. Numerous privacy considerations are a primary feature of the framework and manifest in control measures including but not limited to SSN to employer identification numbers conversions where appropriate, system of records notices, and privacy impact assessments. Complementary to the privacy emphasis are systems ensuring security via controlled data usage and disclosure. These include mechanisms such as IRBs and data use agreements, nondisclosure agreements, and data-sharing agreements. The accuracy, or content quality, of the data comes from having the right incentives and validation processes in place so that analysts and policymakers can be confident in the reliability of what is on hand. For instance, the prerogative to update some dimensions of personal data must be tied to an important outcome for the individual, such as a greater likelihood of promotion, benefit receipt, or future assignment.

Applying the Firewall Framework

The Green Pages pilot program, part of the Army's talent management initiative, is but one example of the potential for the Service to collect, analyze, and use big data to improve officer productivity and satisfaction. The key ideas embedded in the firewall framework were essential to its development and recent Green Pages piloting efforts. Green Pages is a concept that uses a software platform that allows officers to supplement existing administrative records with user-fed data such as hobbies, past experiences, interests, and preferences in the context of seeking out a best-fit assignment. At the heart of the Green Pages concept is the imperative to incentivize and validate the secure collection of accurate, granular, timely, and actionable data; this enables the Army to learn about its on-hand talent inventories while finding optimal employment for its officers. The big data nature of the Green Pages concept cannot be understated: just as the veterans' earnings project discussed earlier combines a variety of existing data, the Green Pages concept integrates administrative data from the Total Army Personnel Database, performance information from officer evaluation reports, and information on civilian schooling and precommissioning experiences. Combining this user-fed information with existing administrative data helps the Army develop a much more complete picture of officer preferences and talents.

For the Green Pages concept to be successful, stakeholders must trust that the organization will keep the data secure and respect individual privacy concerns. These initial imperatives correspond to the key concepts of the firewall framework and thus the entire database sits at the center of the firewall, pillared by privacy and security (see figure 2).

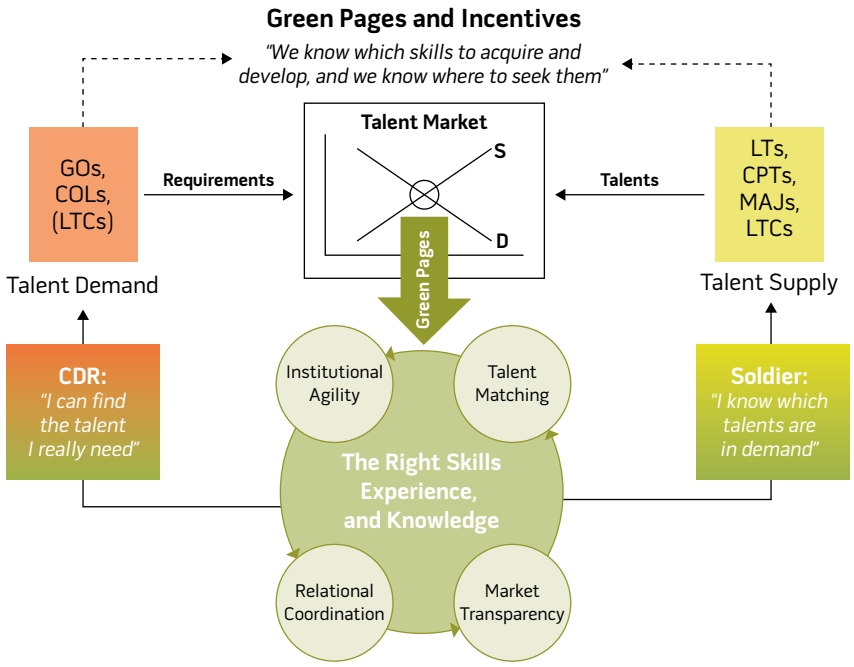
Figure 2. Applying the Firewall Framework to Green Pages



Security is achieved through several features of the Green Pages pilot program. The Web and database servers are configured according to DOD baseline security standards. The servers also use antivirus, host-based firewalls and the DOD Host Based Security System to mitigate known security threats. All Web-based client and server communication is accomplished using appropriate encryption. This secure traffic passes through a reverse Web proxy to conceal the underlying network architecture from potential attackers. A firewall mitigates both injection and scripting attacks. These servers reside within a DOD Data Center with security guards, limited access controlled by Common Access Card (CAC), and security cameras. The database is backed up nightly to network storage. A limited number of system administrators and database administrators have access to the database server and database backups on network storage.

Privacy is achieved through strict authentication procedures and a continuum of what is available at each echelon of profile view. The Green Pages pilot implements authentication using enterprise single sign-on via the Army Knowledge Online (AKO) Single Sign-On. Users gain authentication mostly through CAC/personal identification number with limited use of AKO username/password, where username/password authentication only allows an individual to view her own data. Authorization is controlled by logic built into the Web application. Data access is segmented by role (Headquarters Department of the Army [HQDA], Human Resources Command [HRC], unit strength managers, and users). Within the Web application, users can modify their privacy setting to control the portions of their user profile viewable by others. This does not limit access to their profile by users with higher level roles (HQDA, HRC). At the least restrictive level, strength managers and senior leaders can view basic information such as home address, security clearance, and last change-of-duty station date. Further authorizations enable the user to see the experience overview, current and past chains of command, education, and assignment preferences. Only at the most restrictive echelon can the viewer see full name, email address, current assignment, and organization. Finally, the Green Pages database contains limited PII. To reduce the risk of accidental disclosure, the SSN

Figure 3. Talent Market Enabled by Thoughtful Data Strategy



is replaced with a unique employee identifier, such as AKO username or DOD Electronic Data Interchange number. Similarly, date of birth is replaced with year of birth.

Incentives to maintain the quality of the data are also important to the Green Pages concept; the officer must have "skin in the game" to reveal new elements of the officer's talents and preferences and validate existing information. Whereas in the past officers would receive assignments from the Army without submitting input beyond just their preferences, there is now an incentive structure through the Green Pages market mechanism that is centered on the productive dimensions—or talents—of the officers. We depict this market mechanism in figure 3. Company-grade and field-grade officers represent the supply of talent in this setting, while units represent the demanders of these talents. Optimal talent matches require that both sides of the market have ready access to information that will facilitate matching the right officer to the right position. Within Green Pages, officers (the supply side) are incentivized to reveal their talents while units have a clear incentive to explicitly convey their talent demands. With the proper incentives in place to foster an exchange of accurate, granular, and timely talent data between market participants, the Army collects much better talent data on its officers. Remember that the emphases on security and privacy undergird this entire market information exchange.

Validation is an important feature of the mechanism design for the Green Pages concept. The spectrum of talent-related data is naturally broad because it encompasses anything that measures the officer's potential for productivity. A market-based construct such as Green Pages gives users near instantaneous access to their data. This facilitates validation, corrections, and high-frequency updates to Army administrative data. The fact that peers and mentors can view officer profiles provides an additional important validation mechanism. The linkage between data contained in the Green Pages concept and the assignment process provides perhaps the most powerful validation mechanism of all. For instance, it would not be good for an officer's career if he were hired as a Chinese language expert when the officer's proficiency is actually in Arabic. Thus, the officer has a strong incentive to regularly monitor data in Green Pages and update any information that is incorrect; the result for the Army is validated talent data that is more accurate, granular, timely, and actionable.

A Way Forward

Our nation's military must embrace the fact that big data is here to stay. It must identify methods to tap the vast informational content resident in big data to meet our national security objectives more effectively, while avoiding the negative consequences of uninformed and improper use of this data. Given the importance of trust within these institutions, the stakes are particularly high; misguided uses of this information and potential security breaches of individual data can degrade the morale of Servicemembers and erode public trust in the military.

This article has defined big data and provided a framework for thinking about the ethics of big data in the context of the military. We believe that the firewall framework is one way to orient big data efforts toward security and privacy while incentivizing the provision of accurate and granular data; the firewall provided guiding principles that were useful in the Green Pages case study outlined above. Nonetheless, the firewall framework is simply an initial step in a new area that is still developing and relevant to the military and many other institutions and organizations. Institutions that deal with big data must be mindful to build agility into their formal promises as this is an area of constant change.

Given the vast amounts of data that the military maintains and the high stakes associated with preserving it and ensuring its proper use, the military must engage both internally and externally in the ongoing early dialogues related to the ethics of big data. The military can help to shape the development of the ethics of big data—which will eventually grow into a set of norms with far-reaching implications for both the private and public sectors. Additionally, the military needs to have thoughtful protocols for securing, transferring, storing, and using big data, and must update these protocols with changing technologies. Moreover, the military

GEN Ann Dunwoody, Commanding General of Army Materiel Command, and Mrs. Linda Via promote LTG Dennis Via to rank of general during ceremony at Redstone Arsenal, Alabama, August 2012 (U.S. Army/Teddy Wade)

must continue to refine systems that ensure proper permissions are requested and granted for accessing and using big data. Finally, it must educate the force not only on the proper ethical use of data, but also on the correct use of statistical procedures used to inform decisionmaking. This training must extend to the consumers of analysis so that the military can implement appropriately informed policies. This type of training is crucial for the leaders of tomorrow's military and would be an appropriate feature at all levels of professional military education. **JFQ**

Notes

[1] "What Is Big Data? Bringing Big Data to the Enterprise," *IBM.com*, available at <http://www.ibm.com/big-data/us/en/>.

[2] Kord Davis, *Ethics of Big Data: Balancing Risk and Innovation* (Sebastopol, CA: O'Reilly Media, 2012).

[3] Neil M. Richards and Jonathan H. King, "Big Data Ethics," *Wake Forest Law Review*, January 2014, available at <http://ssrn.com/abstract=2384174>.

[4] President's Council of Advisors on Science and Technology, *Big Data: Seizing Opportunities, Preserving Values* (Washington, DC: The White House, 2014), available at <www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>.

[5] Ibid., 32–34. See the brief discussion of foundational "third-party doctrine" Supreme Court cases and associated statutes, such as the 1974 Privacy Act.

[6] Ibid., 51–53. The recent White House report cautions against the use of big data analysis to enable discrimination such as in this example.

[7] Shvetank Shah, Andrew Horne, and Jaime Capella, "Good Data Won't Guarantee Good Decisions," *Harvard Business Review*, April 2012.

[8] See Charlie Wheelan, *Naked Statistics* (New York: Norton, 2013).

We thank members from the Office of Economic and Manpower Analysis at the U.S. Military Academy for their valuable comments and suggestions to this article. The Office of Economic and Manpower Analysis has maintained one of the Army's single largest databases for more than 30 years and has extensive experience in working with big data.

Aerospace Ground Equipment craftsman remains vigilant over 761 pieces of equipment for MQ-1 Predator and MQ-9 Reaper unmanned aerial vehicles (U.S. Air Force/Christian Clausen)

Activity-Based Intelligence

Revolutionizing Military Intelligence Analysis

By Chandler P. Atwood

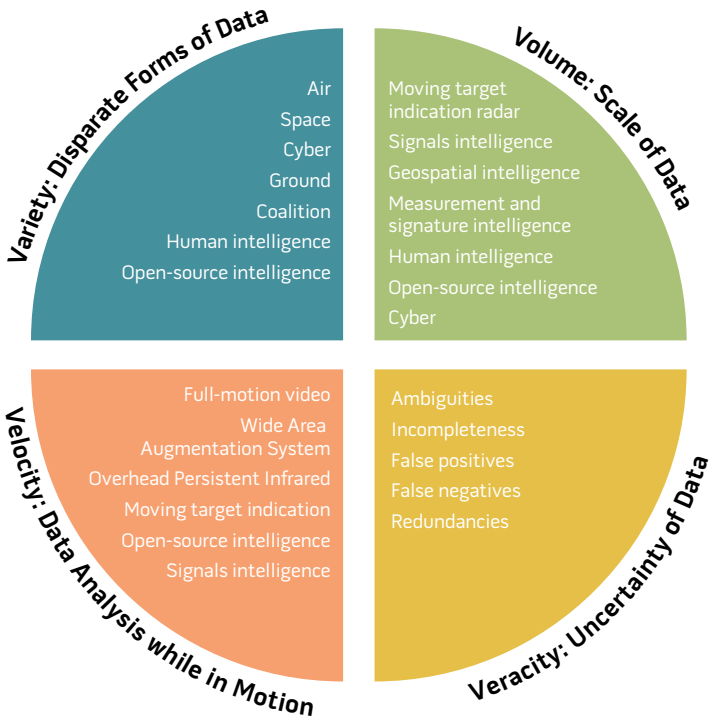
Information-age technology is advancing at a stunning pace, yielding increasingly complex information architectures, data accessibility, and knowledge management—all of which have created the conditions for a leap in intelligence processes," stated Lieutenant General Robert Otto, the Air Force Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance (ISR).[1] The vast amount of information that the Intelligence Community (IC) collects demands a transformation in the way the Department of Defense (DOD) intelligence enterprise processes, organizes, and presents data. The enterprise must embrace the opportunities inherent to big data while also driving toward a unified strategy with the IC. The primary strategy thus far has been acquisition based, looking to industry and research and development organizations to provide the next best tool and software, rather than addressing the more existential requirement of advancing analytical tradecraft and transforming antiquated intelligence analysis and processing methods.

In our current diffuse and multipolar threat environment, the DOD intelligence enterprise faces the daunting task of discerning abnormal and/or

Lieutenant Colonel Chandler P. Atwood, USAF, is Chief of the Commander's Action Group for the Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance. He was previously a National Defense Fellow at The Washington Institute for Near East Policy and Squadron Director of Operations at the National Air and Space Intelligence Center.

significant activities from normal patterns of activities. To truly revolutionize and fundamentally change from an individual exploitation process to analysis-based tradecraft, the enterprise needs to harness the potential of big data, replacing the methodology of individually exploited pieces of data with an activity-based analysis approach, known as Activity-Based Intelligence (ABI). Use of the ABI methodology will enable our intelligence analysts to focus on hard problems with critical timelines as well as normal day-to-day production activities across the spectrum of conflict. This methodology will aid in the development and understanding of patterns of life, which in turn will enable analysts to differentiate abnormal from normal activities as well as potentially defining a "new normal." Furthermore, the sharp incline in the amount of data, recent information technology (IT) advances, and the ABI methodology impel significant changes within the traditional DOD intelligence production model of PCPAD (planning and direction, collection, processing and exploitation, analysis and production, and dissemination).

Figure 1. The Four Vs of Big Data



Big Data: A Problem or Opportunity?

Today's IC faces the data challenges of the "four Vs" with persistent sensors soaking the battlespace: *variety, volume, velocity*, and *veracity*. The DOD intelligence enterprise processing, exploitation, and dissemination (PED) systems and analysts cannot keep pace with the four Vs inherent in big data or continue to mitigate the tendency of each organizational entity to build stovepiped systems with poor interoperability overall.[2] The IC has dealt with data volume and velocity issues for decades, but the challenge has more recently expanded to include the full complexity of big data with variety and veracity added to the equation as illustrated in figure 1.

Even today in Afghanistan where ISR forces have been redundantly layered for years, the creation of a timely, coherent picture gained from integrated, multi-source intelligence data is a rarity. For instance, U.S. and North Atlantic Treaty Organization forces in Afghanistan have suffered losses when they were surprised by an unexpected larger insurgent force not detected and relayed in time even when there were ever-present ISR assets operating in a permissible environment.[3] This assertion still stands true today and portends an enduring DOD intelligence enterprise challenge of integrating disparate datasets into a clear picture for warfighters and their commanders across all types of battlespaces. Whether we reflect over the last 13 years operating in a permissive environment or look to the future in a potentially highly contested battlespace, DOD intelligence organizations will operate in domains in which all four Vs of data combine to create the big data conundrum.

Most DOD intelligence enterprise analysts contend that "drowning in data" leaves our intelligence organizations afflicted with overstimulation and overwhelmed with man-hour intensive PED. Specifically, the DOD Joint Distributed Common Ground System (DCGS) enterprise fits this paradigm and has yet to reach its full potential of networking and integrating the entire spectrum of national and tactical intelligence due to a preoccupation with data exploitation. DCGS is a system with a laser focus on single-source, quick-look reporting. It does not provide larger discovery from the integration of multiple intelligence (multi-INT) disciplines and sources.

Since 2003, the Air Force DCGS and the greater DOD intelligence enterprise have seen a steep growth in the number of sensors with multiple exponential increases in the data each produces, as well as the multiple forms of data formats they must process and exploit. For instance, we started this era with a strong and growing dependence on a narrow field-of-view full-motion video (FMV) MQ-1 Predator observing a 0.1 x 0.1 kilometer (km) "soda straw" spot on the ground. Today our DCGS core sites focus on processing, exploiting, and disseminating intelligence from dozens of MQ-1 combat air patrols while also absorbing increased data from newer sensors with a much larger target area coverage. In the future, wide area airborne surveillance programs of record will have a sensor coverage area of an enormous 30 x 30 km. These advances in motion video coupled with the expansion of sensor

coverage across the spectral bands, such as the data intensive hyperspectral sensors, and the burgeoning light detection and ranging sensors drive a significantly greater data problem concerning the four Vs. The list goes on, with increasing signals intelligence (SIGINT) sensors and moving target indicator (MTI) sensors as well as the growing integration of overhead persistent infrared (OPIR) data and nontraditional measurement and signatures (MASINT) sensors into the IC enterprise. This ever-expanding list of data generators leaves the ISR operators in a state of near paralysis and the training shops and leadership saying, "enough is enough."[4] Today's focus on single-source exploitation in an environment of multisource data availability clearly hinders analysts from understanding and conveying the overall meaning of the integrated results.

In today's dynamic and complex battlespace, the DOD intelligence enterprise requires near simultaneous access to and analysis of data from a multitude of sources and disciplines—thereby embracing big data. These integrated disciplines should include at a minimum SIGINT, human intelligence (HUMINT), geospatial intelligence (GEOINT), MASINT, and even open source intelligence (OSINT) to understand the problem and provide actionable intelligence to warfighters. Today's analysts tend to develop an expertise in only one or two of these disciplines, resulting in their inability to understand and convey the overall meaning of the integrated results potentially obtainable from all data.

In spite of big data overwhelming our existing ISR exploitation capabilities, there are indications that change is starting to occur. The increase in sensors and resulting vast amounts of disparate data coupled with the increasing capabilities of IT systems to handle the deluge are transforming intelligence analysis. The traditional process of stitching together sparse data to derive conclusions is now evolving to a process of extracting conclusions from aggregation and distillation of big data.[5] Although IT solutions will enable our analytical shift, the largest impact will come from replacing the methodology of individually exploited pieces of data with Activity-Based Intelligence. ABI is a high-quality methodology for maximizing the value we can derive from big data, making new discoveries about adversary patterns and networks, yielding context, and therefore also providing greater understanding.[6] The information age now brings the potential for technological improvements to harness big data in such a way that true ABI methodology can indeed become a reality.

Activity-Based Intelligence

Activity-Based Intelligence has already been defined in many different ways, and after many months of debate, a codified and agreed-upon definition, based on Under Secretary of Defense for Intelligence guidance, finally exists: "ABI is a multi-INT approach to activity and transactional data analysis to resolve unknowns, develop object and network knowledge, and drive collection."[7] The following paraphrasing may resonate more with DOD ISR professionals, enabling a better understanding of ABI, though not intending to replace or circumvent the established definition:

ABI is an analysis methodology which rapidly integrates data from multiple INTs and sources around the interactions of people, events and activities, in order to discover relevant patterns, determine and identify change, and characterize those patterns to drive collection and create decision advantage.[8]

ABI is an inherently multi-INT methodology that invokes a transformational approach to data processing and analysis. The methodology uses a large volume of data from a variety of intelligence sources to enable data correlations that, among other things, drive discovery of weak signatures and patterns in a noisy data environment. This methodology will fill critical gaps in single-source data PED processes. It will also help resolve unknowns through the process of correlating activity data with information about the attributes, relationships, and behaviors of known and unknown objects in ways that cannot be done today without proper automation. By accumulating the multi-INT data on individual activities, an ABI analyst can correlate activities, detect anomalies, and discover links between objects. The derived object and network knowledge will enable the discovery of new facilities, links and nodes, and patterns of activity. An ABI analyst correlating activities and resolving objects will enable real-time tipping and cueing of sensors, thereby driving collection, again, in ways that cannot be done today.[9]

Methodology in Action

The confluence of four Vs in big data requires a significantly different way of handling the task(s) that traditional intelligence methodologies cannot support. For instance, the Intelligence Community reportedly had pieces of information that provided indicators of the impending August 21, 2013, chemical weapons (CW) attack in Syria, but seemingly failed to process and integrate the information in time to portend such an attack. According to a White House Press Secretary official report, "In the three days prior to the attack, we collected streams of HUMINT, SIGINT and GEOINT that reveal regime activities that we assess were associated with preparations for a chemical weapons attack."[10] This reported shortfall raises troublesome questions for the analytical integration capabilities of the IC and provides a hypothetical backdrop from which to develop an ABI tradecraft workflow template applying its four pillars and main enablers.[11]

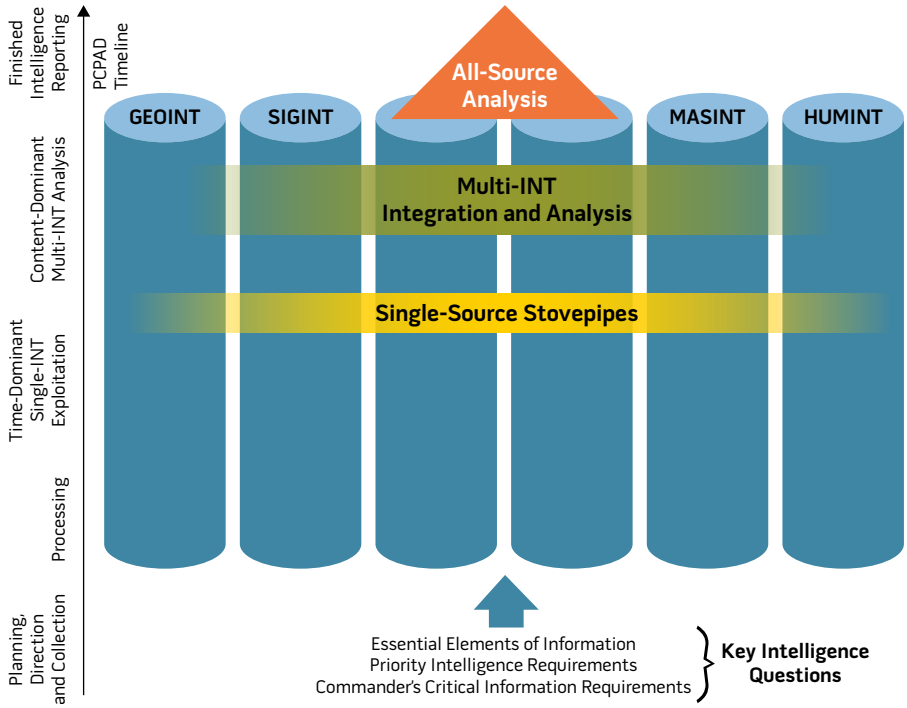
Perhaps the individual agencies had the data 3 days prior but failed to (or were unable to) integrate all the data from their respective data streams in order to first derive understanding and then to identify key indicators of abnormal activity in a way that would lead to a credible, defendable conclusion. Conceivably, the data associated with the individual intelligence components only made sense after the attack, when the events were manually retraced and integrated across the other data sources through a manpower extensive post-event reconstruction.

The ABI methodology will revolutionize the analytic processes applied to situations like this example in a way that will enable automated real-time correlation of data and information from current collections as well as through archived data sources. These data correlations can establish baseline understanding of the information, historic trends of activity, and provide identification of anomalies. When in action, the ABI methodology has four, not necessarily sequential, pillars: georeference to discover, integrate before exploitation, data (sensor) neutrality, and sequence neutrality.[12]

The absolute first step in the ABI methodology must be *georeference to discover*. All data sources should be spatially and temporally indexed at the time of collection rather than treated as an afterthought or last step in the analytic process as often accomplished today across the IC, if possible. ABI depends on a variety of multi-INT data that need to be integrated to fill holes in sparse single-source datasets. To mitigate gaps in single-source data, all of the collected data must be "georeferenced" to a specific point in space and time.[13] Only then will an ABI analyst be able to correlate, integrate, and cluster the multi-INT data around a "spot of interest," enabling the discovery of entities, activities, transactions, and begin to relate them.[14] Having preconditioned data, with explicit spatial and temporal aspects, allows the ABI analysts to spend more time applying contextual knowledge to the problem set, focusing their analysis.

Using Syria's use of chemical weapons as a backdrop, what if regime personnel were observed operating in an area used to prepare chemical weapons in the days leading up to the attack? Hypothetically, we could call this an analysis failure where the IC had the indications but did not integrate and make sense of the incoming multi-INT data fast enough. Imagine instead HUMINT and other data sources not fully used in the analysis had been georeferenced and temporally tagged at collection, enabling an ABI analyst to retrieve and integrate the sources through an interactive spatial application tool.[15] The ABI product then

Figure 2. Traditional and Current PCPAD Intelligence Process



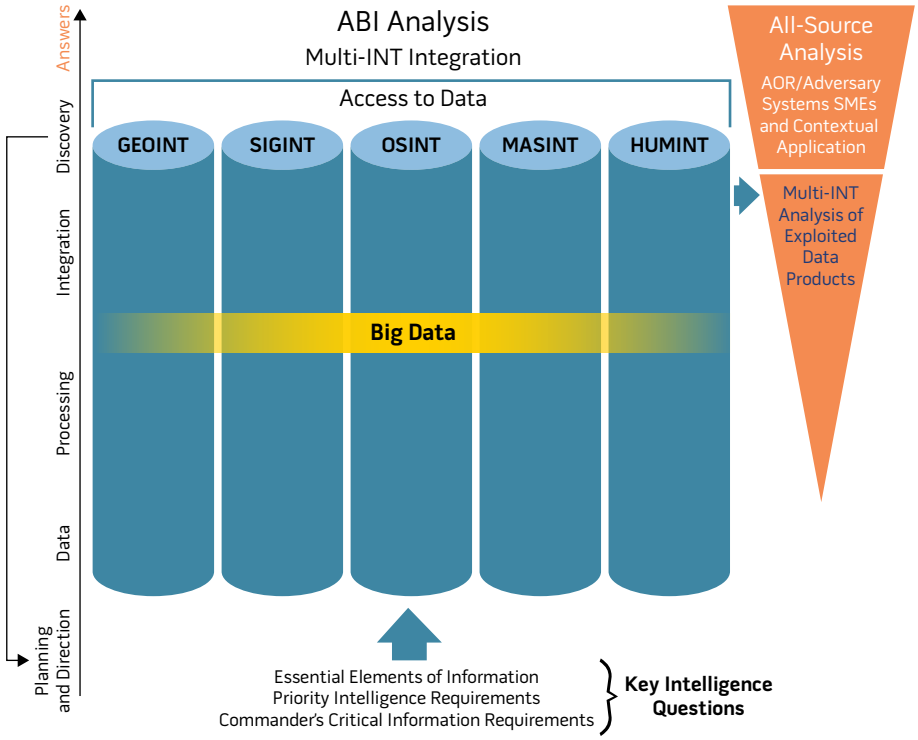
becomes a relationship "map" of the objects and entities and their transactions, such as those activities surrounding preparatory CW attack efforts. Even in contested battlespaces, where data sources are sparse, it is only through georeferencing all the available multi-INT data that the ABI analysts can begin their workflow.

After georeferencing the collected data within the ABI context, it will be *integrated before exploitation*. Georeferenced data are associated at the earliest integration point, before an analyst conducts detailed exploitation and analysis, not at the end of the production process. The ABI methodology looks for relationships at the earliest point of consumption, applying context earlier than in the classic intelligence process. That process, codified in joint doctrine as a production model of PCPAD, integrates exploited and analyzed single-source information at the end of the process.[16] When executed, the PCPAD model narrowly focuses on exploiting the stovepiped data first and then passing to a multi-INT or all-source analyst to integrate the different pieces of exploited data as depicted in figure 2.

Still, much of the IC continues to be mired in a linear process that relies too heavily on a preset targeted collection strategy as well as an independent single-source PED and analysis process to address intelligence gaps. Yet by embracing the ABI methodology, the IC can overcome profound yet surmountable challenges of transforming this antiquated intelligence process and the related analytic tradecraft into one best suited for success in today's data-congested enterprise.

During execution, the PCPAD model narrowly focuses on a linear approach to pushing data, typically single-sourced, to address an intelligence gap driven by causation, like Syria's CW example. In this traditional method, some information may have been inadvertently discounted during the stovepiped exploitation process. In some cases, the relevancy of the information only develops significance when associated and integrated with another data source at the time of exploitation. The ABI methodology will provide the means of avoiding the trap of viewing data from a single source or multiple sources of the same discipline and making what may

Figure 3. How ABI Transforms the Traditional Intelligence Process



well prove to be inaccurate or incomplete value judgments before understanding the full picture.

In so doing, the ABI methodology enables analysts to sift through large volumes and varieties of data to see how the data overlap and intersect, identifying associations and enabling significant events to rise above the noise of data triage. For instance, in our previous CW example, let us now presume a HUMINT or SIGINT tip, not "finished intelligence" reporting, has been intercepted indicating that the use of CW had been ordered. This is information that could have been integrated earlier in the intelligence production process. A GEOINT analyst routinely observing imagery may have not seen abnormal activity days leading up to the attack. However, if the HUMINT or SIGINT tip had been known by the GEOINT analyst at the time of imagery exploitation, then what was potentially disregarded as insignificant activity may have been associated with preparatory CW operations and identified as such.

As depicted in figure 3, this potential ABI-derived discovery would then drive additional analysis including the time-dominant exploitation requirement of the GEOINT, SIGINT, and any additional INT data pertaining to that area. In this case, the time-dominant exploitation of the HUMINT or SIGINT provides the GEOINT analyst with enough insight to focus his exploitation efforts on a specific area of the imagery, potentially reducing exploitation resources. Assuming limited information is available to corroborate potentially anomalous activity, a dynamic re-tasking of sensors could be conducted, driving real-time collection. After the ABI analyst commingles the various pieces of data and identifies key pieces, exploitation begins to occur within each INT, providing the results to the multi-INT analysts to conduct integration of the exploited information and address the intelligence questions as the process continues to add additional information. Finally, an all-source analyst may receive the multi-INT integrated information to provide additional context and subject matter expertise to this ABI methodology discovered intelligence of preparatory CW operations.

In addition to PCPAD's inherent inflexibility to integrate single INT sources earlier in the process, it relies too heavily on an antiquated preset targeted collection strategy against known adversary targets. The PCPAD premise of targeted collection is highly reliant on known and distinguishable signatures supported with doctrinally aligned tactics, techniques, and procedures (TTPs) to be effective against such threats. The post–Cold War's diffuse and complex threat environment displays inherently nonstate threats, fleeting signatures, and minimally supporting doctrine from which to focus PCPAD's target-based collection strategy. To transform the current paradigm from a deliberate fixed target focus requires a revised model.

The ABI methodology does not have a traditional target-centric approach to analysis, like observing specific CW stockpiles and production facilities on a daily basis. Using the *integrate before exploit* ABI pillar, the analyst is informed by the commingled data, allowing him to search for observables and to potentially discover a threat signature or indicator that was not discernable in the PCPAD paradigm. An ABI analyst integrating a variety of disparate datasets in this fashion may have provided the activity linkage leading up to Syria's CW attack well before the intelligence process reached the all-source analyst.

Furthermore, the observed activity, potential discoveries, and identification of gaps surrounding a specific problem set will in turn drive current and subsequent collection requirements as depicted in figure 3, with the arrow from "discovery" to "planning and direction." This correlated data discovery will potentially answer questions that were never asked or the analysts were unaware of the answers or how to answer the question in the past. Accordingly, the collection manager and end customer do not necessarily need to know beforehand how the analysts plan to use the data, unlike the traditional targeted collection model. Such a transformation will likely drive predetermined collection decks obsolete, while also enabling the analysts to improve their understanding and build specialized

Distributed Common Ground System–Army Program Manager assesses tactical glasses demonstrated at Enterprise Challenge 13 (U.S. Army/Kristine Smedley)

collection strategies with faster decision cycles and anticipatory analysis.

The first two ABI methodological approaches of georeference to discover and data integration before exploitation with their focus on multi-INT data clustering can enable the discovery of new intelligence in a noisy data environment. Moreover, these new methods can also fundamentally transform the PCPAD and traditional analytic processes to be more responsive to analyst and warfighter needs.

The next pillar to achieving the ABI methodological transformation occurs only when we take a *data (sensor) neutrality* approach. This pillar is predicated on accepting all data sources—that each can potentially be equally viable and that one data source or piece of data is not biased over the other.[17] In this case, an ABI analyst does not favor any particular intelligence discipline (for example, SIGINT) reporting over any other data source (for example, GEOINT synthetic aperture radar [SAR] imagery). Likewise, an ABI analyst must accept a nonspatial or georeferenced data source because it may act as a tip for other sources. For instance, SIGINT or HUMINT data that may have an error of probability that geographically covers a large city and cannot be pinpointed to a specific suburb or facility must be treated as just as viable as a piece of information with exacting coordinates. Also, a fleeting piece of intelligence, like transitory CW preparations and the nonpersistent nature of poisonous gas when employed, must reside at an analyst's fingertips to correlate with the other pattern developing multi-INT data. Additionally, the data must encompass a full range of sources, to include OSINT, especially social media (for example, YouTube).[18] For instance, local Syrian social media reports of the CW attack numbered in the thousands, with hundreds of videos to confirm the attack and highly credible reporting from international humanitarian organizations and hospitals.[19] Of course, an ABI analyst has to understand and account for the confidence, reliability, and potential errors in the data source as well as the interrelationships of what the data from the separate sources are providing and their integrated results.

Much of the collected data prior to an event or abnormal activity, such as the activity observed 3 days prior to the CW attack, would likely appear irrelevant at the time of initial exploitation. However, the observed CW activity can be quickly identified as significant when an ABI analyst applies the *sequence neutrality* approach, the fourth pillar of ABI. Essentially, ABI analysis of the data may happen immediately, or the data may not become relevant until the analyst acquires more data and is able to develop a pattern of activity.[20] As such, previously collected

(continued on page 32)

Five Examples of Big Data Analytics and the Future of ISR

By Jon A. Kimminau

When we talk about U.S. Air Force intelligence, surveillance, and reconnaissance in 2023, we often depict it graphically as beginning with a global array of sensors that produces a variety of data absorbed in a cloud, from which multisource and all-source analysts produce decision advantage for both national and combatant decisionmakers. Big data analytics is at the core of this vision, and its impacts to intelligence analysts and the way they execute their mission will be multifaceted.

How can we describe these impacts? What are some examples or ways to show how big data analytics will work? To answer these questions, we must first understand what is meant by big data analytics and how it can be distinguished from most of our present analysis operations. There are three essential elements to true big data analytics:

- A high volume, velocity, and variety of data with both time and space dimensions from multiple sources are collected and metatagged in an information "cloud."
- Applications that allow analysts to manipulate, visualize, and synthesize the data, leveraging relationships between data elements, must be dynamically developed and accessible.
- Analyst operations on the cloud—their projects, queries, folders, access—must be captured and continuously added to the cloud as additional metatagged data.

Dr. Jon A. Kimminau is a Defense Intelligence Senior Leader and the U.S. Air Force Analysis Mission Technical Advisor.

These three elements are at the heart of big data applications in the commercial and information technology digital space. But more importantly they are at the forefront of future intelligence developments and will greatly impact every activity.

Discovery

Intelligence discovery is the ability to select, manipulate, and correlate data from multiple sources in order to identify information relevant to ongoing operations and requirements. Discovery is about better organizing and using the data that we already know. It is also about finding previously hidden patterns and anomalies—former Secretary Donald Rumsfeld's "unknown unknowns." Imagine in the future that a Pacific Air Forces air operations center analyst is examining air activity in the South China Sea over the past 2 weeks and notes a pattern of flights from select Chinese bases to outposts in the Paracel and Spratly Island groupings. Using an application, the analyst isolates bases of origin and destination and filters the past 4 months of data to visualize the activity. She discovers a pattern that may be a shuttle operation of troops to outposts from which the troops apparently do not return to home base. This activity is then reported by the analyst as a previously unknown buildup of Chinese forces in disputed islands, which may lead to international confrontation. Our ability to discover this kind of activity today is severely restricted by an inability to understand what we have already got. The data are derived from varying sensors, compiled in separate databases, and not accessible and manipulable by any single application. Big data analytics will help us move to a digital "commons," organize our data in uniform manner across all our sources, and then bring new applications for exploring the data to an analyst's workstation.

Assessment

Intelligence assessment is the ability to provide focused examination of data and information about an object or an event, to classify and categorize it, and to assess its reliability and credibility in order to create estimates of capabilities and impacts. Assessment is how intelligence determines what our consumers should be concerned with—and how concerned they should be. Imagine in the future a military strike against a terrorist target in a Central Asian nation, using an unmanned aerial vehicle. Commanders want to know the success of the strike. An analyst, drawing on near-real-time imagery and past information about the site and activity around it, uses an application that detects all changes. In addition, the application provides a visualization of the reactions of both people and objects in the target vicinity. Synthesizing this information rapidly, the analyst can provide near-real-time battle damage assessment to the commander, reporting that the primary physical target was destroyed, that bodies were present, and that vehicles appeared to take some persons away from the target area at speed. Although communications from the high value individual (HVI) ceased at the strike, the vehicle departure with a body is included in the assessment that "the target was physically destroyed; X persons killed and Y possibly injured; therefore, we are confident the HVI

was injured or killed in the action." At another level, the theater commander is apprised in near real time of the results of several simultaneous strikes, providing an assessment of campaign effectiveness. Our ability to execute both kinds of assessment today is hampered by lack of access to multiple sources, varying levels of security controls, a lack of tools to rapidly correlate and visualize the data, and lack of command and control applications to aggregate the reports into a near-real-time campaign battle damage assessment.

Explanation

Intelligence explanation is the ability to examine events and derive knowledge and insights from interrelated data in order to create causal descriptions and propose significance in greater contexts. Explanation is how intelligence provides our consumers narrative stories, relates events to broader situations, and identifies the core of what is going on. Imagine in the future a U.S. European Command analyst is tasked to look at an incident of civil unrest in southeastern Lithuania. After composing and executing a query and defining an area of interest, the system presents not only information on the event in question, but also that a fellow analyst is looking at a similar event in Estonia and that two other events of the past week are under examination by others. Examining the project folders of these analysts, she then follows a thread about Russian troop movements along the borders and an aerial reconnaissance intercept of a North Atlantic Treaty Organization platform by a Russian fighter. Collaborating with these and other analysts, an intelligence estimate is produced that projects a building confrontation of Lithuanian and Estonian separatists with host countries and potential provocation by Russian border elements. This type of assessment is difficult to produce today as data and information sets are often segregated by type of source and regional assignment. In addition, while analysts can collaborate today, it is more often a "pull" system where one asks those who are known to be working a problem, rather than a "push" system where analysts may be automatically alerted to other similar work. Big data analytics expands the avenues for collaboration and multidisciplinary, shared expertise in a global, distributed enterprise.

Anticipation

Intelligence anticipation is the ability to warn and describe future states of the environment based on the manipulation and synthesis of past and present data. Anticipation includes near-term warning and longer term forecasting to alert and prepare decisionmakers to events relevant to their responsibilities. Imagine a Central Air Forces analyst whose responsibility is force protection surveillance of remaining U.S. bases in Afghanistan. Years of experience and lessons learned by the Joint Improvised Explosive Device Organization have been incorporated into system alert templates for a warning application. These templates respond to a variety of intelligence and open-source inputs when activated and focused on designated areas. When a large vehicle being towed on a major road near one base apparently stalls, sufficient indicators in the template create a warning for the analysts of a potential massive car bomb situation. The analyst reports the alert to base leadership and security teams, and protocols are followed to isolate and assess the vehicle. This kind of anticipatory intelligence is possible today only when collection resources are focused to deployed exploitation centers, and analysts there have both attention on the situation and the personal experience to look for appropriate indicators. Big data analytics can incorporate that experience into applications, cast the security net far wider, and recognize potential situations much quicker.

Delivery

Intelligence delivery is the ability to develop, tailor, and present intelligence products and services according to customer requirements and preferences. Delivery is about both intelligence products—from tactical reports to full-blown finished intelligence estimates—and intelligence services, ranging from crew threat briefings to daily intelligence assessments at headquarters to real-time analyst response to requests for information. Imagine a flag officer in a theater combatant command position reading a classified daily briefing on a digital pad. One item deals with a past day event of a U.S. reconnaissance platform being intercepted by an adversary military fighter. The senior leader then taps an icon titled "recent recce [reconnaissance] intercepts" and is provided a list of both local and global intercepts for the past six months. Noting several in his own area of responsibility, the leader also taps an icon titled "recent provocative incidents" and discovers several ship confrontations in international waters and an intelligence estimate and open news media editorial both assessing the increased provocations as being intended to influence an upcoming Secretary of Defense military visit. The ability for a consumer to draw on the context of an intelligence report service for a broader variety of relevant information exists only in a limited fashion today—dependent on extensive, manual preparation of the background data and hyperlinks to it—but a big data infrastructure can automate the foundational background analytics.

Big data analytics offers the potential to revolutionize how analysis supports our warfighters and national decisionmakers with intelligence—the decision advantage in national security. This revolution extends across the spectrum of intelligence analysis activity—from discovery and assessment, to explanation and anticipation, to delivery. JFQ

(continued from page 29)

and archived multi-INT data analyzed in a forensic manner can be as or more important than data obtained near real time.[21] Additionally, an ABI analyst will not be biased toward an archived dataset that was specifically part of the targeted collection deck. In fact, incidentally collected data may be as or more significant than data collected in a targeted fashion. In some cases, data may need to be reexploited and analyzed based on additional information or may be repurposed for a different target within the same collection window.

Establishing the ABI Methodology

The described examples reveal how ABI methodology provides insight earlier in the intelligence process, enabling analysts to spend more time gaining context and analyzing the problem, while machine-to-machine processing interfaces and correlates the georeferenced data automatically. This new paradigm, as reflected in figure 3 (with flipped pyramid), reveals how the DOD intelligence enterprise could shift its model of exploiting approximately 80 percent of the collected data to one focused only on the pertinent 20 percent.[22] By analyzing only the pertinent information and focusing the PED efforts, there will be a net manpower and cost savings to answer the key intelligence questions in an ABI-enabled and discovery focused environment.

The DOD intelligence enterprise must avoid the temptation to focus purely on acquiring the next widget or-specific toolset and focus first on developing the proper big data–enabled analytic environment. Although these developmental ABI toolsets will be invaluable to eventually executing the methodology, the first foundational step for DOD to derive maximum value from its data must be to ensure that the sensor collection-to-analysis timeline is quick enough to detect a pattern. This process must take place in a matter of minutes to be truly actionable by a warfighter, not days (as seen in today's multi-INT analysis paradigm). To accomplish this, the architecture must be able to scale to the level required to retrieve and transmit the vast new and old data sources and store the datasets efficiently for extended periods of time for archival analysis.

Available technologies such as the Cloud and High Performance Computing with advanced algorithms have matured rapidly and may provide the proper solution space to handle the data storage dilemma and processing of complex datasets that enable ABI. However, the Cloud and High Performance Computing do not completely resolve the requisite architecture and bandwidth requirements to transmit and retrieve large disparate datasets from the sensor to the analyst in a timely fashion.

The time is right to move toward an integrated DOD and national intelligence enterprise architecture "with budget realities, current state of technologies and a sense of urgency in the IC leadership all combining to create an optimal climate for positive change," according to the IC Chief Information Officers in an IC Information Technology Enterprise (ITE) white paper.[23] In 2012, the Director of National Intelligence moved to transform a historically agency-centric IT approach to a new model of common architecture—labeled IC ITE, which will provide the IT shared services model for the national IC. The five leading national intelligence agencies—Central Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, Defense Intelligence Agency, and National Reconnaissance Office—have combined efforts to move the community to a "single, secure, coherent, mutually operated and integrated IC IT Enterprise."[24] With over 70 percent of the IC under DOD, the IC and DOD have ideally paired to share a common vision and have a similar timeline and path ahead to ensure a broader intelligence enterprise approach. The DOD and IC share the same vision but are working on parallel solutions that are not necessarily creating a completely integrated intelligence enterprise with analytical transparency—allowing a seamless collaborative environment.[25]

The Defense Information Systems Agency (DISA) has been charged with the herculean task of consolidating and integrating multiple DOD networks into one common, shared network known as the Joint Information Environment (JIE). Ostensibly, the JIE currently faces the challenge of interacting and competing DOD program offices and being funded only by participants who desire increased IT efficiencies. Furthermore, the IC ITE task force recently stated that the JIE "is neither an enterprise (requiring common mission and leadership) nor an architecture (requiring tight management of implementation)."[26] In fact, Admiral David Simpson, DISA Vice Director, pointed out that the JIE "is not a program of record or a joint program office."[27] This troubling state of affairs suggests that DOD should reexamine the JIE and the end-goal of creating a common, integrated network when it does not include complete DOD buy-in, and more important, is not in sync with the IC ITE construct. This two-pronged approach with both JIE and IC ITE will drive many DOD intelligence organizations to pick between the two or, even worse, to have to develop a hybrid system that interacts with both. In fact, the Air Force ISR 2023 strategy contends that to handle the challenges of data overflow and to transform to an ABI methodology, the Air Force ISR enterprise must be a "full partner of the IC-ITE and JIE."[28] This approach portends an enterprise with uncommon IT services, disparate architectures, and an untenable budget during a more constrained economic environment.

Conclusion

Using the four-pillared approach, ABI will provide solutions to assembling an answer by fitting small bits of linked yet disparate information from brief ISR windows into a complete picture. This will enable analysts to pull meaningful images from a sea of pictures, enabling discovery and greater context across the fabric of data for subsequent analysis. The success of ABI relies on the inte-

gration and correlation of truly large amounts of multi-INT data, as well as the tools to handle and appreciate what the ABI methodology is revealing. Many analysts coming out of operations in Iraq and Afghanistan presuppose that ABI is only enabled by persistently collected data, like ubiquitous full-motion video, on activity and transactions over a broad area. However, ABI truly harnesses big data by using a variety of integrated sources regardless of sensor platform. Even in contested battlespaces such as the hypothetical CW example, ABI does not necessarily depend on 24/7 sensor coverage—it builds on a variety of multi-INT data that can be integrated to fill holes in sparse single-source datasets.

The DOD intelligence enterprise must look over the horizon to an ABI analytic environment where such ISR sources as streaming FMV, MTI, OPIR, SIGINT, MASINT, SAR, spectral, and thermal imagery are integrated at the post-processed and georeferenced entry point and compared with archived collected data in an automated fashion. By harnessing a new IT environment enabled by ABI methodologies, analysts will be able to rely on readily available high-speed machine-to-machine processing and big data to make ABI possible on a large scale. These intuitive concepts will require significant effort and a unified IC strategy to overcome the technical and cultural challenges of developing such an information-sharing environment and paradigm-shifting approach to the traditional intelligence process.

During the Cold War, the IC had a laser focus on the adversary and became adept at distinguishing and even predicting Soviet strategic bomber activity and surface-to-air missile TTPs because they possessed discernable signatures, and those signatures were embedded in doctrine. Today, the IC faces more dynamic and multifaceted adversaries that possess fleeting signatures and minimally supporting doctrine. The DOD intelligence enterprise must collectively invest in the ABI tools, develop analyst tradecraft, and embrace a transformed intelligence process to repossess this level of understanding. Only then will we be able to address the near peer countries and asymmetric threats, exhibiting weak and nonpersistent signatures for tactical and strategic production needs. **JFQ**

Notes

[1] Robert P. Otto, *Air Force ISR 2023: Delivering Decision Advantage* (Washington, DC: Headquarters Department of the U.S. Air Force, 2013).

[2] Lydia Ines Rivera, Debbie Salierno, and Allen Siwap, "Multi-Intelligence Distribution Architecture," Capstone Team Project, University of California, San Diego, 2013.

[3] Michael W. Isherwood, *Layering ISR Forces*, Mitchell Paper 8, (Arlington, VA: Mitchell Institute Press, December 2011).

[4] John K. Langley, "Occupational Burnout and Retention of Air Force Distributed Common Ground System (DCGS) Intelligence Personnel," RGSD-306 (Ph.D. diss., Pardee RAND Graduate School, 2012).

[5] Michael Farber et al., *Massive Data Analytics and the Cloud: A Revolution in Intelligence Analysis* (McLean, VA: Booz Allen Hamilton, 2011).

[6] Letitia A. Long, "Activity Based Intelligence: Understanding the Unknown," *The Intelligencer* 20, no. 2 (Fall/Winter 2013), 7–15.

[7] David Gauthier, "Activity-Based Intelligence Definition for the Intelligence Community," National Geospatial-Intelligence Agency, 2013.

[8] Jon Kimminau, author interview, October 18, 2013.

[9] Gauthier.

[10] "Government Assessment of the Syrian Government's Use of Chemical Weapons on August 21, 2013," The White House, August 30, 2013.

[11] Shane Harris et al., "U.S. Had Intel on Chemical Strike Before It Was Launched," *Foreign Policy*, August 30, 2013.

[12] Gauthier.

[13] Mark Phillips, "A Brief Overview of Activity Based Intelligence and Human Domain Analytics," *Trajectory*, 2012.

[14] Gauthier.

[15] Ibid.

[16] Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations* (Washington, DC: The Joint Staff, 2012).

[17] Gauthier.

[18] Kristin Quinn, "A Better Toolbox: Analytic Methodology Has Evolved Significantly Since the Cold War," *Trajectory* (Winter 2012), 1–8.

[19] "Government Assessment."

[20] Quinn.

[21] Gauthier.

[22] Robert Jimenez, presentation, Big Data for Intelligence Symposium, Defense Strategies Institute, November 2013.

[23] Accenture, "Driving High Performance in Government: Maximizing the Value of Public-Sector Shared Services," The Government Executive Series, January 2005; Terry Roberts et al., White Paper, "Intelligence Community Information Technology Enterprise: Doing in Common What Is Commonly Done," Intelligence and National Security Alliance, February 2013.

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] Amber Corrin, "JIE's Murky Progress Raising Questions," *FCW* [Federal Computer Week], August 27, 2013.

[28] Otto.

Innovative, modular unmanned flight research vehicle X-56A allows investigation of active flutter suppression and gust load alleviation technology (U.S. Air Force)

The Defense Innovation Initiative

The Importance of Capability Prototyping

By Edie Williams and Alan R. Shaffer

The recently unveiled Defense Innovation Initiative aims to "pursue innovative ways to sustain and advance our military superiority for the 21st Century" by finding "new and creative ways to sustain, and in some areas expand, our advantages even as we deal with more limited resources."[1] This double-edged sword of producing cutting-edge technology at a time when budgets are declining may seem counterintuitive but actually has some historical precedent:

The U.S. changed the security landscape in the 1970s and 1980s with networked precision strike, stealth, and surveillance for conventional forces. We will identify a third offset strategy that puts the competitive advantage firmly in the hands of American power projection over the coming decades.[2]

Dr. Edie Williams is a Consultant for the Assistant Secretary of Defense for Research and Engineering. Mr. Alan R. Shaffer is Principal Deputy to the Assistant Secretary of Defense for Research and Engineering.

Developing game-changing technology during periods of declining budgets requires two main ingredients. The first is building a culture of innovation with scientists, engineers, and midgrade military officers that fosters thinking about old problems in new ways. The second, most important ingredient is having senior leaders and bureaucrats who open the way for innovation through support of experimentation and prototyping. This article outlines two historical examples of successful military innovation efforts, the current challenges facing the Department of Defense (DOD), including the complexity of the national security environment, the decline in research, development, test, and evaluation (RDT&E) budgets, and finally, in spite of these challenges, the DOD strategy for developing innovative military capabilities moving forward.

A Rich History

DOD has a rich history of innovation through prototyping for the development of future military capability. Two of the best historical examples, tank prototyping and X-planes, illustrate different characteristics of what makes prototyping successful. Tank prototyping was driven by the imperative to find an alternative to embedded trench warfare tactics used in World War I. These efforts emerged from midgrade military officers driven by ideas for new tactics and employment techniques who challenged industry to develop technology that would facilitate their ideas. X-planes were driven by timely application of the development of turbine jet engines by innovative scientists and engineers working with military personnel. The process involved nearly continuous insertion of new technology operating inside an established paradigm shared by DOD and industry. This collaboration allowed new tactics and employment techniques to be developed based on the information learned through the development.

Tank Prototyping and Experimentation. A well-researched and documented example of capability prototyping and experimentation is the integration of tanks into the mechanized combat arms of the U.S. Army from World War I to the beginning of World War II. According to Robert Cameron, the "Mechanized Force emerged as a tactical laboratory intended to determine the optimal organization and doctrine for a combat unit built around the tank."[3] As profound a statement as this sounds, tank development during this period was met with every possible level of resistance, hamstrung by limited budgets and overshadowed by an enormous amount of parochialism. A brief but deeper look at the emergence of tank technology during and between World War I and World War II also reveals the efficacy of capability prototyping that resulted in spite of the obstacles and resulted in victory over Axis forces in World War II and later the emergence of the most sophisticated mechanized force the world has ever seen.

In early World War I, the British and French had each built, and were both using, tanks.[4] The British used tanks to overcome obstacles to the infantry whereas the French used tanks as fire support to complement the firepower of the infantry.[5] The U.S. Army saw merit in both uses but had no documented requirements or plans to build any until after the war. They partnered with the British and French armies to learn about the new tank technology without committing to production of any American variants.

In February 1918, General John J. Pershing activated the Light Tank School in Bourg, France, and appointed a young officer, George S. Patton, to lead the school and experiment with tactics, techniques, and procedures (TTPs).[6] Near the end of the war in 1918, another young officer named Dwight D. Eisenhower was sent to Camp Meade, Maryland, to plan for the creation of the first tank battalion.[7] The collaboration and passion for tank warfare between these two icons would last throughout their careers and result in the dominance of Allied tank warfare in Europe and North Africa in World War II. Early on, though, Patton and Eisenhower argued against conventional TTP wisdom and for using tanks as a separate arm of the fighting force not merely in support of the infantry. They opined that the lack of enthusiasm for tanks was due to "inadequate knowledge of [their] use and potential."[8] In addition to developing and experimenting with tanks at Camp Meade, Eisenhower and Patton did a great deal of writing about tank warfare and tank design in the *Infantry Journal*—nearly always going against the grain of Army leadership.[9]

After World War I, Army leadership, supported by Congress, disbanded the small tank units being used for experimentation and subordinated the few tanks that were left to the infantry. Eisenhower and Patton continued to experiment with tanks and develop doctrine and TTPs to use them as a separate combat arm. When the research and development funding was cut to nearly zero, however, both officers were reassigned and the development of tanks stagnated.[10] Continued funding austerity only allowed one tank prototype to be built between 1925 and 1931.[11]

In the shadow of the edict set forth by Congress in the 1920 National Defense Act, which subordinated tanks to the infantry, there was increasing agreement that tank development needed to continue in spite of the bureaucratic maze set up by the War Department and Congress. Brigadier General Samuel Rockenbach, formerly Chief of the Tank Corps and Commandant of the Tank School, saw promise in the ideas of Eisenhower and Patton, so he kept tank development and experimentation alive.[12] But it was not until after a trip to visit with the British army's Experimental Mechanized Force in 1927 that Secretary of War Dwight Davis finally established the American Experimental Mechanized Force at Camp Meade in 1928.[13]

In 1930, when Douglas MacArthur was made Chief of Staff of the Army, he began an effort to mechanize the force with a particular emphasis on tanks. He also supported Patton and Eisenhower's ideas about offensive uses of tanks and sponsored some limited experimentation efforts to keep the momentum going. Just prior to World War II, Eisenhower became a trainer and author of the winning battle plan for the newly established Louisiana Maneuvers, which were[14]

pre-World War II General Headquarters exercises initiated by General George C. Marshall to prepare the Army for World War II. They featured the field-testing of new doctrinal and organizational concepts, and of new equipment and schemes for its employment. They provided practical, hands-on experience in leading troops in the field with the most modern of configurations. They force-fed change to an institution that otherwise was only beginning to shake off its prewar somnolence.[15]

The Louisiana Maneuvers during 1940–1941 were intended to change a peacetime mentality and prepare the Army for the impending global conflict.[16] Marshall was determined to use experimentation to design a fighting force that had expertly trained Soldiers following sound doctrine in ways that fostered "innovation and growth in extraordinary ways."[17]

Fifty years later, General Gordon R. Sullivan, Army Chief of Staff, came into office "confronted with a number of conditions that greatly taxed the Army: the end of the Cold War; large, congressionally mandated reductions in Army funding; concomitantly large reductions in the size of the force; and a series of contingency deployments."[18] He took a lesson from Marshall and established the modern Louisiana Maneuvers (LAM) to ready a force that could fight in the 21st century with agile and innovative capabilities. His modern version of Marshall's idea was based on "iterative experimentation that would make extensive use of computer-based simulations to test proposed doctrine, procedures, organizations, and equipment."[19] Some of the most important capabilities that came out of LAM, including Total Asset Visibility, Battlefield Digitization, and Owning the Night, are ones that have paid dividends many times over.[20]

Lessons learned from the introduction of tank technology during and between World War I and World War II and the larger experimentation efforts of both the original Louisiana Maneuvers and the modern Louisiana Maneuvers after the first Gulf War are applicable to the situation we face today following many years of war in Iraq and Afghanistan. The circumstances in both historical cases and in our current situation are the same: declining defense budgets, shrinking force levels, limited research and development funding, and doctrinal and political debates about the character of warfare in the future.

The first lesson to be learned is that with limited resources, prototyping and experimentation are good investments. A second lesson is that doctrine based on past wars is not usually valuable when preparing for future conflicts. The final lesson is that there are always young men and women such as Eisenhower and Patton in our ranks who have creativity in their DNA. They should be allowed to share it within a system that supports agility and innovation.

Evolution of X-Plane Prototyping and Military Aviation. An equally well-known series of prototypes in military history are the X-planes. In a brochure specifically published to share the results of the first X-plane prototype with industry, the purpose for the research was explained as follows:

The limited knowledge of aerodynamics and flight performance in the transonic and supersonic speed ranges possessed in 1944 dictated the initiation of research projects which would increase our meager fund of fundamental and factual information in this field of learning. A comprehensive program for the development of purely research aircraft was laid down and a maximum effort was directed toward its immediate implementation (emphasis added).[21]

A purpose statement like this could be written for any of the technological challenges we face today. The key elements are limited knowledge of the technology, clear mandate, and understanding that the primary intent is for research.

In response to its stated purpose, the X-1 program, which lasted from 1946 to 1958, developed seven airframes, flew 236 test flights, and experienced only three major accidents. The accomplishments of the X-1 series were not only noteworthy at the time but also provided an important array of technologies that can be found in nearly all high performance military aircraft today. In addition to being the first aircraft to break the sound barrier in level flight, the X-1 series of prototypes set a baseline of high-speed and high-altitude testing and proved the aerodynamic viability of thin wing sections.[22]

During the 1950s, 17 other X-plane projects were launched to test everything from tail-less airframes to vertical takeoff and landing (VTOL). By way of illustration, the X-14 series tested VTOL technology from 1957 to 1981 and paved the way for the X-22 series (1966–1984) that eventually developed the dual-tandem ducted propeller configuration found in the V-22 aircraft of today. An example of X-plane prototyping during this period that did not result in production or even a testable prototype was the X-6 (1955–1957), which was designed to test the feasibility of using nuclear propulsion in an aircraft.[23]

During the 1960s, seven more X-plane prototyping projects produced testable aircraft. Although many other technologies were matured during this period, two notable programs were the X-23A (unmanned) that tested ablative materials for hypersonic reentry vehicles used in the space program and the X-26 series that made significant contributions to stealth designs that would later be produced in some of the most sophisticated reconnaissance aircraft ever produced. The 1970s only produced one X-plane program, whose unique contribution was that it was a home-built aircraft designed to explore the usefulness of small seaplanes for civil police patrol in Southeast Asia. Like the decade that preceded it, the 1980s produced only one X-plane, which is notable because it introduced the forward-swept wing design, advanced composites, and other aerodynamic advances that allowed it to fly supersonically.

These developments paved the way for all high-performance fighter aircraft in production since that time. The final decade of the 20th century also produced only one full-sized X-plane, the X-31 (1990–1995) Extremely Short Takeoff

X-2 rocket plane dropped from B-50 Superfortress mothership in mid-1950s (NASA)

and Landing thrust vectoring super maneuverability test bed, along with three other scale models that were used to explore other design modifications.

In the first decade and a half of the 21st century, activity in the X-plane community increased with X-32 to X-56 series producing unmanned combat air vehicle demonstrators, compound helicopter Vectored Thrust Ducted Propeller technology, and a hypersonic scramjet. Several of these projects were tied directly to the Joint Strike Fighter and F-22 aircraft development programs.

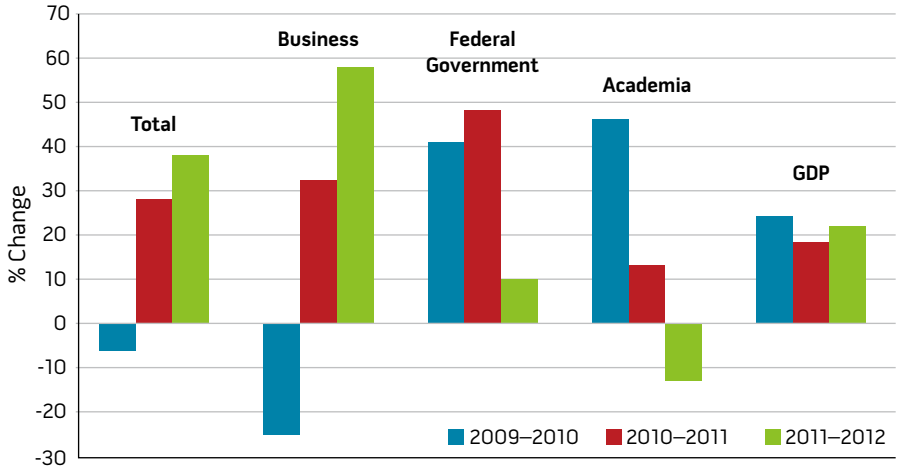
When all 56 X-plane programs are plotted on a chart from 1940 to 2012, several findings emerge. First, it takes several decades of prototyping for some technologies to end up in a fielded aircraft. Second, during periods of increased war spending (for example, the Cold War and Iraq and Afghanistan wars), fewer prototypes are built. Finally, X-plane programs in recent decades are more aligned with program development than the "purely research" aims of the X-1 program.[24]

X-plane prototyping highlights two potential benefits that can inform the offset strategy being employed in the Defense Innovation Initiative. The first and perhaps most compelling benefit of using prototyping for future capability development during budget uncertainty is that it provides a way to keep pace with technology without having to commit large sums of funding to traditional acquisition programs. The second benefit of prototyping as a cost-sharing mechanism is that it provides a way to partner with industry in an environment that offers open exchange of information.

Current Challenges

As evidenced by the tank and X-plane examples, development of innovative warfighting capability in the 20th century was driven by the need to obtain and maintain superior technology-based capabilities. From low observables to space to precision munitions, the United States has maintained a significant military advantage over its adversaries through innovative technologies. Current trends in global security combined with political and financial pressures, however, are forcing DOD to reexamine how it develops operational capability in a cumbersome acquisition process that developed during the

Figure 1. Business Soars, Academia Sinks
(Changes in U.S. GDP and R&D, by performer in constant 2005 dollars)



Source: National Science Board, Science and Engineering Indicators 2014 (Arlington, VA: National Science Foundation, 2014).

Cold War. The combined pressures of complex threats and significant defense spending reductions are compelling DOD to make bold strategic choices in its approach to developing capability that maintains technical superiority.

In his February 24, 2014, testimony on the fiscal year 2015 budget, Defense Secretary Chuck Hagel concluded, "we are entering an era where American dominance on the seas, in the skies, and in space can no longer be taken for granted."[25] Deputy Secretary of Defense Robert Work added, "the United States has never, since the end of World War II, tried to match our potential adversaries tank for tank, airplane for airplane, person for person, missile for missile. We have always sought an offset."[26] The new offset strategy is based on encouraging a culture of innovation in our people and our business practices, that is, the "creation of a long-range research and development program" that produces breakthrough technology, as well as the "reinvigoration of wargaming" and prototyping that develops new operational concepts.[27] Two significant challenges to the strategy, however, are the complexity of the national security environment and the increasing fiscal pressures on the DOD budget in general and more specifically the RDT&E budget.

Complexity of the National Security Environment. Complexity of the national security environment is defined by increasing challenges from nation-states and nonstate actors who challenge the security of the United States and its allies in the domains of land, sea, air, space, and cyberspace. This confluence of challenges includes:

- increasing pace of technology development that challenges our ability to keep up when constrained by 20th-century planning and budgeting processes
- growth of the importance of warfighting enablers such as space, cyberspace, and electromagnetic spectrum
- decreasing budgets and procurement
- the "Power of One" where one person can disrupt large, complex systems with knowledge and tools widely available on the Internet
- system-of-systems dependencies that can be disrupted by breaking the "weakest link."

Other nations are already taking advantage of the increasing pace of technology development by targeting our warfighting enablers and attacking the fragility of our information networks allowing leakages of critical information.

As we emerge from years of war in Iraq and Afghanistan, the geopolitical landscape in the Middle East continues to change, with unrest in Egypt, chemical weapons concerns in Syria, and the persistent nuclear ambitions of Iran leaving the overall situation unstable at best. Additionally, threats from the continuing spread of terrorism across continents continue to challenge the security of not only the Nation but also partner nations and the relationships we are building with our partners. Finally, other nations' development of advanced military capability is closing the capability gap with nations that were well ahead technologically in the past. These complex and growing threats are making strategic choices more difficult.

Fiscal Pressures on Research and Development. Declining budgets are also changing the way we think about developing warfighting capability. Deputy Defense Secretary Work recently made it clear that future budgets will impact capability development:

The national security of the United States is not well served by sequestration. We just have to keep pointing out that if you want a budget-driven strategy, go to sequestration. If you want us to have a strategy that's good for the nation, then go more with the president's budget.[28]

A common indicator of concern in the commercial and Federal Government R&D sectors is rate of growth of R&D compared to the per capita growth of gross domestic product (GDP). The National Science Foundation (NSF) tracks this metric, among many others, and found that from 1989 to 2009 Federal spending for R&D grew just 1.3 percent annually while GDP rose 2.4 percent annually.[29] More recent data from the NSF also show an interesting trend when Federal Government R&D is compared to business R&D. According to the National Science Board Report for 2014, "Most of U.S. basic research is conducted at universities and colleges and funded by the federal government. However, the largest share of U.S. total R&D is development, which is largely performed by the business sector. The business sector also performs the majority of applied research."[30]

Figure 1 illustrates clearly that from 2009 to 2012, business R&D made a dramatic turnaround while Federal Government R&D was in decline. Of concern to DOD is the symbiotic dependence of academic researchers on Federal Government funding and the effect of the reductions in 2011–2012 as noted by the National Science Board. This implies that any DOD solution provider should review industry R&D first and use what industry has already funded, modified to defense needs as appropriate.

The good news is that the 5 percent boost in national R&D spending in 2011 to $428 billion and a jump of 5.7 percent to $452 billion for 2012 are well ahead of the 4 percent growth in the GDP in each of those years.[31] This trend suggests a return to historical patterns in which the Nation's total R&D investment grows at a faster rate than GDP.

DOD has traditionally relied on its RDT&E budget to generate new capability to ensure military superiority. Figure 2 illustrates that RDT&E accounts are contracting sharply since their peak in fiscal year 2009. Procurement budgets are used to complete the development of new capability through systems engineering and manufacturing of weapons systems that exploit the capabilities that have been developed through the RDT&E phases. Figure 3 shows that when the procurement accounts used for new systems development and modernization of current systems are added to RDT&E funding, the calculus of fiscal constraint does not change; in fact, it exacerbates the severity of the situation.

Implications for the current fiscal environment cannot be understated. The reduction in RDT&E accounts will not only cut the investment in new science and technology but will also result in a decline in scientists and engineers working on DOD problems. This decline will result in less national security technical capacity. Pressures on procurement budgets will lead to fewer new start efforts and increased focus on preserving and evolving current capacities. Without strong management, there is a potential for two serious negative impacts. First, there will be a limited appetite for risk that biases decisionmakers against the development and insertion of new technologies. Risk aversion will reduce the pace of technological advance in U.S. programs and permit our global competitors to take advantage of the increasing pace of technology. The second impact of falling RDT&E and procurement budgets will be a reduction of industrial design capability as infrequent new design efforts may

Figure 2. DOD RDT&E Total Obligational Authority for Fiscal Years 1962 to 2014

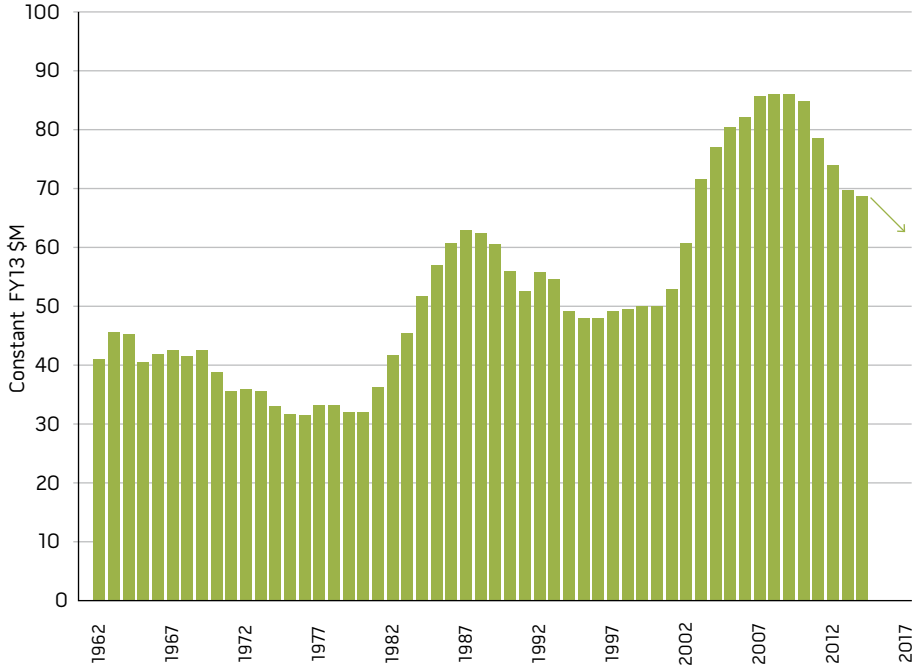


Figure 3. DOD Procurement and RDT&E Total Obligational Authority for Fiscal Years 1962 to 2014

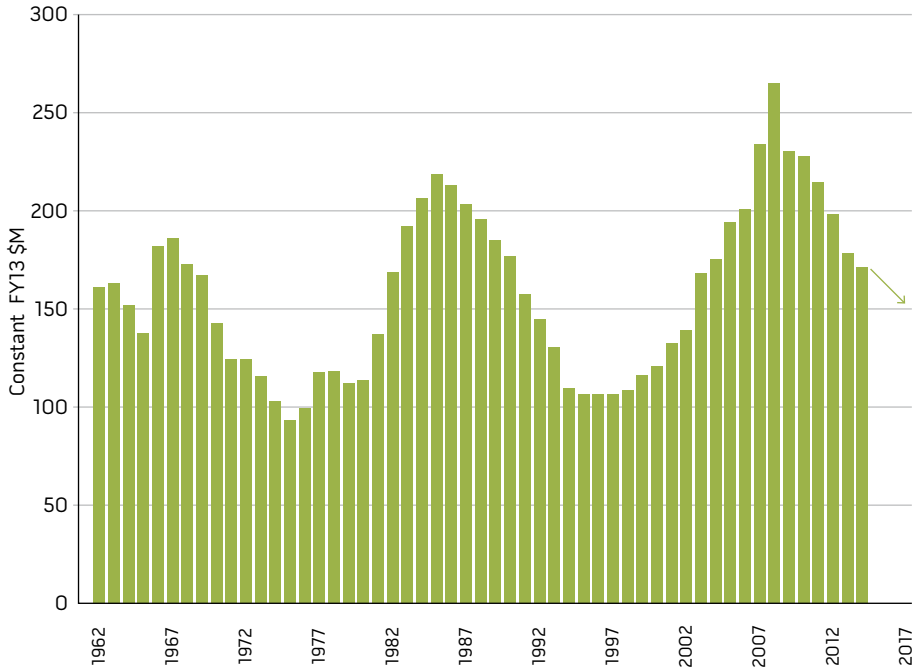
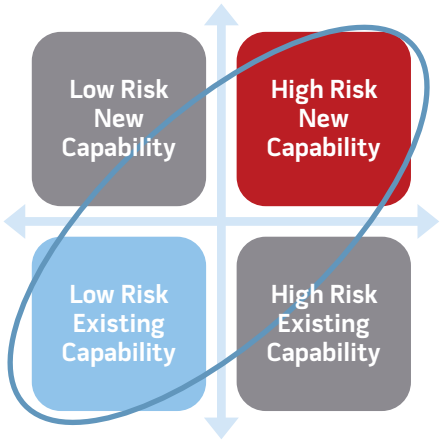


Figure 4. Capability Development Risk Framework



place cutting-edge design capability at risk. It will be difficult to regenerate these defense-specific design capabilities at a later date when they might be required.

Strategy for Innovation Based on Risk

The DOD strategy, as stated in *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, is to "encourage a culture of change and be prudent with its 'seed corn,' balancing reductions necessitated by resource pressures with the imperative to sustain key streams of innovation that may provide significant long term payoffs."[32] In light of a complex set of threats and declining resources for RDT&E and procurement, the challenge faced by DOD is how to sustain and grow investment in future technologies and systems concepts in a period of declining resources. Strategic guidance for how to approach this challenge is contained in the companion document to *Sustaining U.S. Global Leadership*. The *Defense Budget Priorities and Choices* guidance outlines an approach to achieving significant savings over the next 5 years that will result in a joint force that may be "smaller and leaner" but "will remain agile, flexible, ready, innovative, and technologically advanced."[33] Regarding the protection of new capabilities and investments, the guidance directs "increasing funding for a few capabilities while protecting others at existing levels or making comparatively modest reductions" by making "deeper offsetting reductions in areas of lesser priority."[34] The focus of capability development based on risk is illustrated in figure 4.

Capability development under this strategy focuses on two opposite applications of new technology: low-risk applications of new technology that enhance current capability, and high-risk applications of new technology that result in new capability. Developing low-risk applications of new technology to enhance current capability is a path well worn in DOD. We have a rich history of incremental improvement. The challenge at hand, when faced with declining budgets and technologically sophisticated adversaries, is how to protect the "seed corn" or emerging science and technology that could yield breakthroughs in the ways we fight and win wars in the future.

A recent report compiled by the World Technology Evaluation Center, funded and supported by participants from the NSF, National Institutes for Health, National Aeronautics and Space Administration, Environmental Protection Agency, Office of Naval Research, and Department of Agriculture, suggests a useful framework for thinking about the complexities of how to capture emerging science and innovation in the 21st century.[35] The report uses a convergence-divergence cycle for capturing megatrends in science and engineering. The report defines *convergence* as "the escalating and transformative interaction among seemingly distinct scientific disciplines, technologies, communities, and domains of human activity to achieve mutual compatibility, synergism, and integration, and through this process to create added value and branch out into emerging areas to meet shared goals."[36] In the convergence phases of the cycle, a creative phase captures the synergism between multidisciplinary domains and integrates them during the fusion phase. In the divergence phases, the fused knowledge is integrated through systems development in innovative new ways, culminating in the outcome phase where added value applications are tested and deployed.[37]

The report notes that cellular technology, or more specifically the smartphone, provides perhaps the best example for understanding the cycle of convergence and divergence. Combining new knowledge in materials science, nanotechnology, cognitive science, and human-machine interface technologies gave us the cell phone platform approximately a decade ago, but the more recent explosion of applications was fueled by the divergence phases of innovation and outcomes that use the technology in ways that have "profound implications for and secondary impacts on areas as diverse as national security, education, and cognitive science."[38]

Convergence of Scientific Knowledge. The table summarizes the findings of the report titled *Convergence of Knowledge, Technology, and Society: Beyond Convergence of Nano-Bio-Info-Cognitive Technologies* regarding emerging scientific knowledge that could be of interest to DOD.[39]

Thinking in terms of this framework of convergence and divergence, DOD intends to maintain current levels of RDT&E investment and increase investment in warfighting enablers through prototyping for agility and innovation. Convergence will be primarily incubated in the science and technology community while increased commitment toward divergence will be promoted in the engineering, testing, and acquisition communities. Both will require a culture of change and innovation.

Using Capability Prototyping to Maintain Technical Superiority**.** In a recent meeting of senior DOD leadership, the Assistant Secretary of Defense for Acquisition and the Acting Assistant Secretary of Defense for Research and Engineering teamed up to propose an agility and innovation effort aimed at the development of capability through the expanded use of developmental and operational prototypes. Developmental prototypes demonstrate a capability without worrying about operational factors. Operational prototypes demonstrate a capability while taking into account sustainability, manufacturability, and reliability. The combined efforts of the

research and engineering community and acquisition community aim to increase investment in prototyping that will build enabling capabilities such as enhancements to the electromagnetic spectrum and alternative options in space that enhance more conventional programs. Given the direction to move forward, a pilot effort targeted at streamlining the process for proposing, evaluating, and executing agile and innovative prototypes efforts began last year within existing programs of record.

Today's Prototyping for Agility and Innovation. Key to encouraging a culture of change as outlined in *Sustaining U.S. Global Leadership* and the Long Range Research and Development Planning Program is a commitment to "encourage innovation in concepts of operation."[40] In DOD, concepts of operation are developed through experimentation typically combining the use of existing systems and new technology inserted to either existing systems or in the form of prototypes. Military users can exercise prototypes to evaluate opportunity afforded by innovative platforms, systems, and weapons to explore the tactical and strategic advantages offered by new technologies. The advantage of full- or near-full-scale prototypes is their availability to participate in exercises or contingency operations permitting Service leaders to assess their use in an operational context. Experimenting with prototypes in operational environments will provide insights that inform future requirements and provide opportunities to consider systems approaches that represent significant departures from current material solutions. We can leverage developmental and operational prototyping to:

- foster innovation and hedge against technical uncertainty
- preserve industrial base capabilities
- impose strategic costs on potential future adversaries
- explore innovative, technology-enabled military capabilities in a fiscally constrained procurement environment.

There are three elements of our agile and innovative prototyping strategy:

Table. Areas of Emerging Knowledge of Interest to Department of Defense

Foundational Knowledge	Applications	Related technologies
Nanotechnology	Dielectric function, nanoelectronic devices	Optics, photonics, nanomaterials, nanocrystals
Biotechnology	Synthetic biology, genomics	Biological sciences, DNA gene-sequencing
Information technology	Cyber-infrastructure, collaboratories, virtual organizations	Sensors, robotics, quantum computing, citizen science
Cognitive science	Noninvasive brain imaging, embodied robotic systems, brain-mapping	Human-machine interface, big data, cloud computing, medicine
Environmental science	Global climate modeling, weather prediction	Biofuels, water management, space
Human health and physical potential	Regenerative medicine, advanced prosthetics, performance enhancement	Bioethics, nanotechnology for single-cell analytics, vaccines
Quantum engineering	Precision timing, information technologies	Remote sensing
Manufacturing	Additive manufacturing: 3D printing, robotic prosthetics	Small-scale multifunctional machines

- establish dedicated developmental and operational prototyping projects of significant scope and limited duration to design, develop, and deliver full-scale operational prototypes of cutting-edge land, sea, air, and space systems
- deliver operational prototypes to joint and Service users to exercise and evaluate military utility under realistic conditions alongside current capabilities
- use knowledge and experience obtained from these prototypes to develop new warfighting concepts and inform requirements and technical feasibility of future acquisition programs.

Key characteristics of an effective prototyping program are the ability to remain rapid and agile, visible and public, and fair and open. The ability to be rapid and agile will be facilitated by design cycles (inside of 2 years) that are short enough to permit rapid and continuous technological advance permitting U.S. capability options to grow faster than a potential opponents cycle time. To ensure visibility, advanced prototyping demonstrations will be unclassified to the greatest extent possible. Demonstrated capability will serve to modify potential adversary's behavior by demonstrating U.S. capabilities and imposing costs on an adversary to develop and deploy counters to U.S. potential capabilities. To remain fair and open, DOD investments in prototyping will create intellectual property that should be shared with largest possible U.S. community. While the government will retain intellectual property rights to technologies developed under prototyping efforts, the knowledge and experience developed will be shared across the defense industrial base. Our desire is not to have prototyping efforts overly influence competitive field for future acquisitions. Prototyping serves as a means for DOD to maintain and technologically refresh critical defense industrial base design and manufacturing capabilities during new start design and production lulls. Delivery of full-scale (or near-full-scale) prototypes can exercise production-representative manufacturing capabilities and supports capital investment in maintaining state-of-the-art design and fabrication capability.

Prototyping also inspires innovative designers and engineers. Providing a conduit to address critical DOD challenges through prototyping should attract the best and brightest in the defense industrial base workforce. Prototyping efforts should also aid in recruiting young scientists and engineers and serve as an important platform to emphasize the

Soldiers abandon disabled M-3 tank during Third Army Louisiana Maneuvers at Camp Polk in 1943 (Signal Corps/Calvano)

attractiveness of science, technology, engineering, and mathematics education. Advanced prototyping efforts also serve as a critical development tool for recruiting and retaining technical leaders already in DOD—these are the programs that careers are built on and inspire others to pursue technical excellence within government service. Finally, public interest in advanced technology prototyping will reflect well on DOD technical capabilities and acquisition workforce.

Conclusion

In a fiscal climate where DOD will be constrained in its pursuit of modernization-focused new starts, developmental and operational prototyping can serve as the means to advance the current state of the possible, exercise cutting-edge design teams, maintain technical advantage over potential future adversaries, and permit operational users to gain insight into future technology-enabled strategies and tactics. In a fiscally constrained environment, it will be critical to avoid thinking of advanced prototypes as lead systems for follow-on procurement programs. Instead, prototyping programs might only be pursued to the point where they provide a realistic exercise of a design concept or its associated manufacturing capabilities. These programs might also demonstrate potential solutions to emerging technological and operational challenges.

To protect "seed corn," DOD must stay abreast of scientific trends and emerging technologies. New discoveries in emerging technologies such as embodied robotic systems and 3D printing could mean unprecedented breakthroughs in defensive and offensive capabilities. Using vision-inspired basic research leads to emerging uses beyond known applications and results in new ideas and inventions that can be nurtured through developmental prototyping. Using a convergence-divergence paradigm, DOD is embarking on a two-pronged, risk-based strategy that uses our resources (funding, facilitates, and people) in the most efficient and effective means to support the defense of

the Nation. Key to this new strategy and supporting the convergence-divergence evolutionary process is our increased emphasis on developmental and operational prototyping.

Whether prototyping is used to develop new and innovative capability or improve existing capability, the efficacy of using it during a period of constrained resources and geopolitical uncertainty is sure. Taking the art of the possible and turning it into the science of the doable is a research and development agenda that is worth pursuing. The success of our efforts, however, will depend on building a culture of change, innovation, and collaboration. The final and most important ingredient will be the intellectual curiosity and creativity of our people. **JFQ**

Notes

[1] Secretary of Defense Memorandum, "The Defense Innovation Initiative," November 15, 2014, 1, available at <www.defense.gov/pubs/OSD013411-14.pdf>.

[2] Ibid., 2.

[3] Robert S. Cameron, *Mobility, Shock, and Firepower: The Emergence of the U.S. Army's Armor Branch, 1917–1945* (Washington, DC: Center for Military History, 2008), 1, available at <www.history.army.mil/html/books/Mobility_Shock_and_Firepower/CMH_30-23-1.pdf>.

[4] Ibid., 2.

[5] Ibid., 3.

[6] Ibid., 3.

[7] Ibid., 9.

[8] Ibid., 11.

[9] Thomas D. Morgan, "Ike and the Tank," available at <www.west-point.org/academy/malo-wa/archive/IkeTank.html>.

[10] Cameron, 22.

[11] Ibid., 25.

[12] Morgan, 4.

[13] Cameron, 32.

[14] Morgan, 5.

[15] James L. Yarrison, *The Modern Louisiana Maneuvers* (Washington, DC: Center for Military History, 1999), i, available at <www.history.army.mil/html/books/Modern_Louisiana_Maneuvers/The_Modern_Louisiana_Maneuvers.pdf>.

[16] Ibid., 2.

[17] Ibid., vi.

[18] Ibid., iii.

[19] Ibid., vi.

[20] Ibid., ix.

[21] U.S. Air Force, *Supersonic Research Airplane XS-1*, Report No. 1 (Washington, DC: NASA Historical Reference Collection, January 9, 1948), available at <http://history.nasa.gov/x1/afsrax.html>.

[22] Rebecca C. McCaleb and Donna L. Holland, *X-33 Environmental Impact Statement: A Fast-Track Approach* (Huntsville, AL: National Aeronautics and Space Administration, January 1, 1998), available at <http://ntrs.nasa.gov/search.jsp?R=19990099294>.

[23] Ibid.

[24] U.S. Air Force.

[25] "Remarks by Secretary Hagel and Gen. Dempsey on the fiscal year 2015 budget preview in the Pentagon Briefing Room," transcript, February 24, 2014, available at <www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5377>.

[26] Jake Richmond, "Work Explains Strategy Behind Innovation Initiative," *DoD News*, November 24, 2014, available at <www.defense.gov/news/newsarticle.aspx?id=123708>.

[27] Ibid.

[28] Ibid.

[29] Rafael Reif and Craig Barrett, "Science Must Be Spared Washington's Axe," *Financial Times*, February 25, 2013, available at <www.ft.com/cms/s/0/14e4e522-7f7d-11e2-97f6-00144feabdc0.html#axzz3QbnVJBaq>.

[30] National Science Board, *Science and Engineering Indicators 2014* (Arlington, VA: National Science Foundation, February 2014).

[31] Mark Boroush, "U.S. R&D Resumes Growth in 2011 and 2012, Ahead of the Pace of the Gross Domestic Product," NSF 14-307, National Science Foundation, December 2013, available at <www.nsf.gov/statistics/infbrief/nsf14307/>.

[32] *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: Department of Defense, 2012), 8.

[33] *Defense Budget Priorities and Choices* (Washington, DC: Department of Defense, January 2012), 1, available at <www.defense.gov/news/Defense_Budget_Priorities.pdf>.

[34] Ibid., 9.

[35] Mihail C. Roco et al., eds., *Convergence of Knowledge, Technology, and Society: Beyond Convergence of Nano-Bio-Info-Cognitive Technologies.* (Lancaster, PA: World Technology Evaluation Center, Inc., 2013), 1.

[36] Ibid., 1.

[37] Ibid., 13.

[38] Ibid., 15.

[39] Ibid., 360–366.

[40] *Sustaining U.S. Global Leadership*, 8.

Princeton University professor has found way to alter property of lone electron without disturbing trillions of electrons in its immediate surroundings, an important step toward developing future types of quantum computers (Courtesy Princeton University/Brian Wilson)

The Quantum Leap into Computing and Communication

A Chinese Perspective

By Cindy Hurst

A nation's success in military operations often rises and falls on the basis of how well it communicates. When a nation does not secure its communications effectively, its enemies intercept and read its communications and win thereby military and diplomatic advantages.[1]

Vice Admiral Noel Gayler, former director of the National Security Agency, once wrote, "Important as it is in peacetime, communications security becomes even more important in wartime."[2] For a few decades, nations have been relying on encryption systems to protect a wide variety of computerized transmissions ranging from commerce to government to mil-

Lieutenant Commander Cindy Hurst, USNR, is an Analyst with the U.S. Army's Foreign Military Studies Office.

itary communications. While today's encryption systems are considered reasonably secure, the possibilities of quantum cryptography and quantum computing offer a whole new dimension and threat to computerized secrecy.

China is among a growing number of countries seeking to unlock the science of quantum cryptography and computing, which many experts believe will one day revolutionize computerized security. With China's ongoing push to modernize its military and advancing to become a global innovative force, success in this area could materialize into an enormous economic and military advantage.

This article examines the significance of these technologies, China's progress in quantum communication and quantum computing, and the consequences for the United States and other nations should the Middle Kingdom acquire a real capability in this science. It is an area that U.S. analysts will need to follow closely in the coming months and years.

China's Leap

The world is currently in the midst of a second quantum revolution.[3] The first quantum revolution began in 1900 when the new rules governing physical science were discovered. Today, in the second quantum revolution, these rules are being used to develop new revolutionary technologies. Two such possible technologies are quantum computing and quantum cryptography, the latter falling within the area of quantum communications. While they each rely on the properties of quantum physics, their end goals differ. Theoretically, a quantum computer would be able to break current encryption systems, but quantum cryptography is arguably unbreakable even by a quantum computer.

The Quantum Computer: Code Breaker or Problem Solver? The idea of creating a quantum computer has been around since the 1970s. These computers would be extremely powerful since they can harness quantum properties. Unlike an ordinary computer, which uses binary numbers (1s or 0s) to represent data, a quantum computer would use quantum bits (qubits), which can simultaneously have the value of 0, 1, or any "superposition" of the two.[4] The quantum phenomenon becomes even more bizarre when considering the concept of "entanglement." Entanglement links the properties of two or more qubits together. These qubits, even when separated, remain strongly correlated or interconnected in a manner much stronger than any classical relationship. This is what famed physicist Albert Einstein called "spooky action at a distance." A quantum computer using entangled qubits would therefore be vastly faster than the average computer, which uses simple binary numbers. Theoretically, once a quantum computer comes online, it would be able to break current encryption systems such as Rivest, Shamir, and Adleman (RSA), a commonly used computer encryption and authentication system that uses a complex algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. These encryption systems are needed to protect information such as financial transactions as well as military and government communications.

In 2001, Guo Guangcan, an academician of the Chinese Academy of Sciences, established the Key Laboratory of Quantum Information at the University of Science and Technology of China (USTC) in Hefei. The laboratory became "the most important research center of quantum information in the country."[5] In January 2006, while the field of quantum technology was still considered in its infancy in China, Guo predicted that the first quantum computer would likely be developed in the next 15 to 20 years.[6] In 2007, Dr. Pan Jianwei, director of the Division of Quantum Physics and Quantum Information at Hefei's National Laboratory for Physical Sciences at the Microscale, USTC, optimistically predicted that the country might be the first to develop a quantum computer.[7] More recently, however, Pan seems to have shifted his focus. A 2010 article quoted him as saying that quantum communication is "more important for China because it is already closer to application" than developing a quantum computer, although the latter is still "very attractive to me."[8] If Pan really did shift his focus, it could be that the reality of the challenges involved with building a quantum computer had indeed set in.

Dr. Ivan Deutsch, professor and Regents' Lecturer at the University of New Mexico, explained the difficulty in achieving a quantum computer. In quantum cryptography, which is explained more in depth below, the goal is to distribute two shared secret keys. Basically, the secret keys are created using the properties of quantum randomness. It works on a particle-by-particle basis. In other words, in quantum encryption one photon can be sent at a time. It is simple to control a single particle. Quantum computing, on the other hand, is much more complex because it deals with computation as opposed to the transmission of single photons. Computations require logic, and logic requires the use of many 1s and 0s that cannot be sent individually since each one is interdependent. Furthermore, each qubit needs to be in an entangled state simultaneously. Due to this added degree of complexity, quantum computing is much further away from realization than quantum cryptography.[9]

Despite this apparent shift in interest from quantum computing to quantum cryptography, in February 2013, a Chinese report emerged touting a breakthrough in trying to achieve the quantum computer: "The solid-state quantum research crew from the University of Science and Technology of China succeeded in performing the quantum logic gate operation on one single electron at 10 picoseconds, renewing the previous world records by nearly 100 times."[10] Prior to China's achievement, "U.S. and Japanese research institutes achieved the electrically controlled semiconductor logic gate at 1,000 picoseconds."[11] China's achievement, however, increased the operational speed by nearly 100 times to 10 picoseconds. According to Guo Guoping, director of the research project:

China has launched the solid-state quantum chip project in efforts to gain a

foothold in the global competition in the next-generation computer chips. . . . The quantum chip . . . will make the quantum computer characterized by exponentially increased operational speed and greatly improved data processing capabilities.[12]

The ability to break current encryption systems makes modern day information vulnerable. Furthermore, an inherent risk to national security should a quantum computer come online would be its ability to access archived information previously protected by systems such as today's RSA encryption. Dr. Jonathan Dowling, a professor and Hearne Chair of Theoretical Physics at Louisiana State University, explained that information encrypted using RSA could be intercepted and archived today in its encrypted format. Once a quantum computer is online, it could be used to break older archived encrypted data, possibly still classified.[13]

Carl Williams, chief of the Quantum Measurement Division of the National Institute of Standards and Technology, agrees that there are certain risks to quantum computers, but he adds that there are benefits as well, pointing out they could eventually solve problems of profound scientific and technical benefit. "If you ask me 100 years from now what the benefit of this technology is, I would probably say it is a societal benefit," stated Williams.[14]

Quantum Communication: The Pursuit of the Perfect Encryption System. Encryption methods have evolved over time, becoming increasingly complex and difficult for an adversary to break. The trend in cryptography has evolved from traditional manual enciphered and deciphered codes to mechanical encryptions and computerized cryptography. Today's top cryptography systems such as RSA and Pretty Good Privacy are considered highly secure. Breaking messages has become nearly impossible with the growing sophistication of today's cryptography. However, experts believe it is only a matter of time before existing encryption systems are broken.

Currently there are projects in place to try to counter the threat of a future quantum computer. Post-quantum cryptography is a relatively new field in which research is conducted on public-key encryption systems, which are not breakable using quantum computers. Quantum cryptography (distinct from post-quantum cryptography) offers another way to try to counter the risks of a quantum computer coming online. This newest form of cryptography is based on quantum theory and is proving to be unbreakable.

Quantum key distribution (QKD), a process within the context of quantum cryptography, generates a random encryption key shared by the sender and recipient. The biggest advantage of QKD is that if a third party attempts to intercept it, the party will be detected and the secret message will not be sent. QKD deals with photon states and works as follows: Alice, Bob, and Eve are three fictional characters. In quantum cryptography, Alice wants to send a secret message to Bob. She has to first send him the key through the process known as QKD. This means she is sending him a series of photons in random quantum states. If Eve tries to intercept the message, it changes the quantum states of the photons.

QKD is already a reality, although limited in capability. A small number of commercial companies have offered quantum encryption systems. For example, the U.S.-based technology company MagiQ sold a system in 2003 called the Q-Box. The Q-Box is a single-photon-based system developed for further research related to QKD. These systems, however, are far from perfect and have had a limited distribution. Moreover, QKD can be sent either via fiber optic or through free space. Going through fiber optic cables, it generally cannot travel more than 50 kilometers (km) without a quantum repeater, which has not yet been developed.

China has touted a number of successful experiments in the area of quantum communication. For example, in 2004 the Key Laboratory of Quantum Information reportedly completed a 125-km fiber point-to-point QKD experiment. This experiment, according to Chinese reports, "solved the problem of stability in quantum cryptography systems."[15] These results are questionable, but not impossible. According to Carl Williams, "If I wait long enough and my fiber is perfectly dark and still, I can probably get a photon through at a longer distance than 50 kilometers."

In a November 2005 article, China claimed to lead the United States, France, and Austria in quantum entanglement research when it provided an "experimental demonstration of five-photon entanglement and open-destination teleportation."[16] The more photons that can be successfully entangled, the higher the accuracy of the transmission.[17]

In 2006, China reported having fulfilled quantum teleportation of a two-particle system. Voting results at the Chinese Academy of Sciences showed that 565 academics chose it as the ninth most significant development that year in the country's science-technology sector.[18]

In 2007, a report stated that China had created a quantum router, which they claimed was the first in the world. The router was said to have succeeded in encrypting data flowing between four computers on a commercial communications system. The router is different from point-to-point transmissions conducted in other parts of the world because it makes a quantum network possible.[19] Then, in May 2009, a report emerged in the Chinese press claiming that the country had built the world's first quantum encrypted government network and that its trial operation in Wuhu City, Anhui Province, served eight government departments in Wuhu.[20]

Scientists in China in 2012 reportedly teleported multiple photons 97 km across a lake within the country.[21] This significant experiment puts China one step closer to achieving global transmission of quantum communications. Scientists would eventually like to use satellites to achieve global transmission of quantum communications. The distance that a quantum key can be sent through free space depends on which direction it is traveling. Traveling straight up toward space, it can go farther due to the integrated air mass (that is, the air becomes less dense). China recognizes that "by

using satellites, ultra-long-distance quantum communication and tests of quantum foundations could be achieved on a global scale."[22]

By 2016, China plans to launch the first "Chinese Quantum Science Satellite," a satellite dedicated to quantum experiments, which according to *China Daily* would put the country ahead of both the United States and Europe. According to Pan, "The satellite will provide scientific answers to the feasibility of intercontinental quantum teleportation—to make it simple, whether I can talk to my friend in Vienna from Beijing on a quantum phone."[23]

Matthew Luce, a researcher with Defense Group Inc.'s Center for Intelligence Research and Analysis, thinks that because of important applications for satellites as well as the security level:

quantum communication technology figures centrally in the objectives of the Chinese military to upgrade their growing command and control capabilities. A functional satellite-based quantum communication system would give the Chinese military the ability to operate further afield without fear of message interception.[24]

Furthermore, Luce points out that China's research in quantum applications could help the country expose weaknesses in a network should the United States or another nation win the race in achieving the same technology.[25]

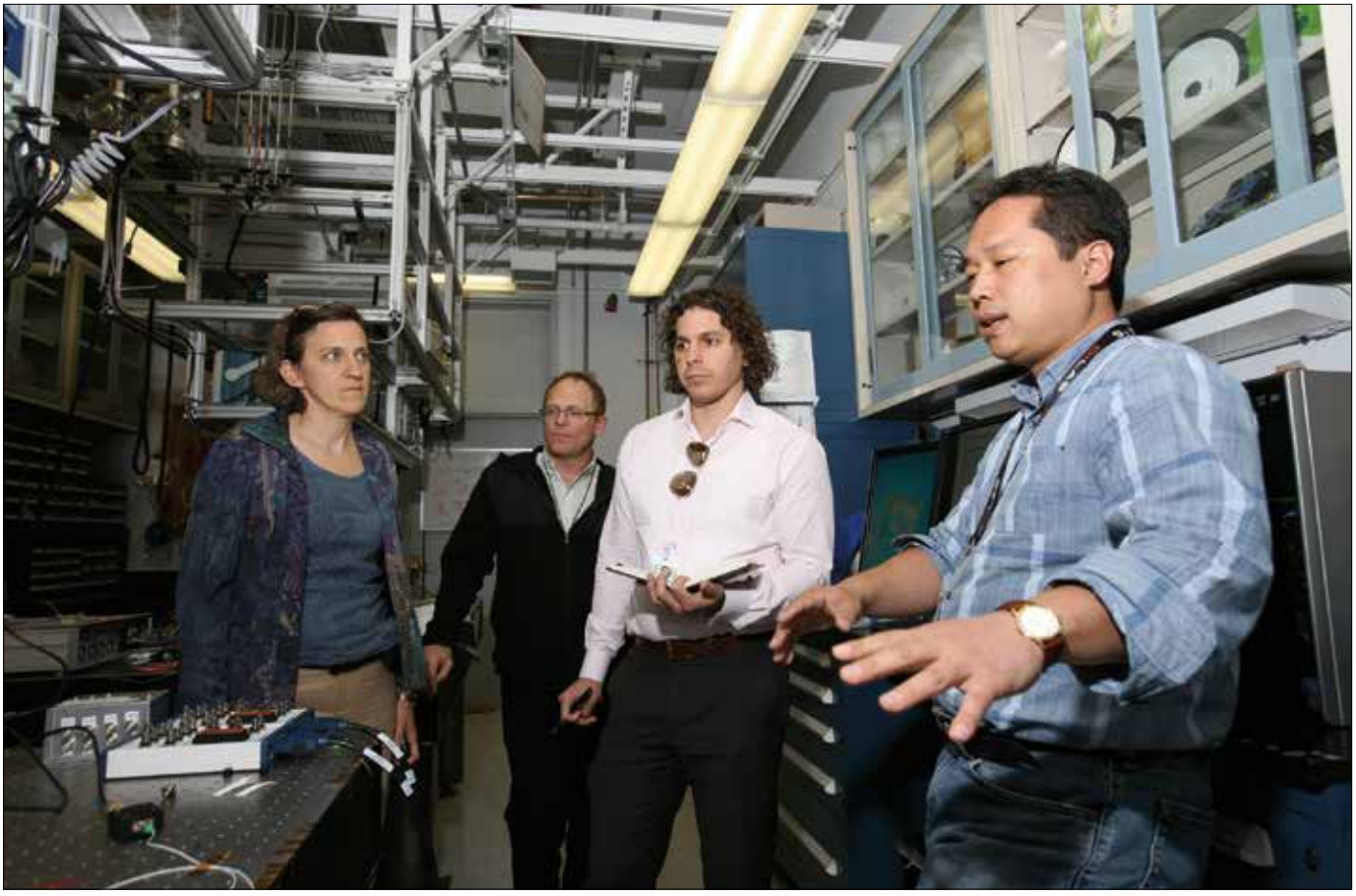
A Military Perspective on Quantum Power

While the possibility of cracking quantum technology is often viewed by scientists in academia as a personal challenge—presenting a potential opportunity to receive a Nobel Prize or a patent—it is also viewed by militaries and governments as having great security potential and significant implications.[26] In November 2012, for example, the U.S. Army News Service reported that scientists at the U.S. Army Research Laboratory were conducting research and development on data teleportation to one day achieve secure, tamper resistant security. According to Ronald Meyers, who is leading an Army project in collaboration with the Joint Quantum Institute at the University of Maryland at College Park, "The greatest potential that a quantum communications network holds for the Army is secure communications." Meyers also contends, "Quantum computers will be able to easily decrypt communications that are currently secure. . . . That's one reason why it's vital for us to explore quantum encryption." Meyers envisions a future in which there will be "very powerful quantum computers with a lot of intelligence. They'll be able to work over long distances without being intercepted. It's going to change the world."[27]

Air Force Research Laboratory Directed Energy Directorate researcher and leader of joint AFRL and University of Hawaii Manoa quantum computing group received two new tabletop quantum computing systems to trap and study behavior of atoms in their condensed, pristine state (U.S. Air Force)

China has also recognized the potential power of quantum communications, and there is evidence indicating it is researching the possibilities at a higher level. Reports reveal that the National University of Defense Technology has been conducting quantum information technology research since the 1990s.[28] The People's Liberation Army (PLA) has clearly taken an interest in quantum communications because other institutions are also studying the topic. For example, the PLA's University of Science and Technology (PLAUST) reportedly opened 11 new research directions in 2011, to include quantum communication technology.[29] Some researchers believe that quantum communications, along with cloud computing, intelligence optic networks, and high-speed satellite communications, provide asymmetric operational superiority for military forces and generate new types of combat power.

PLAUST has worked with both military and nonmilitary research institutes, achieving major successes in key technologies. The university conducts strategic cooperative research with civilian institutes to establish joint laboratories, which have



Sandia National Laboratories' Daniel Soh, right, offers overview of continuous variable quantum key distribution lab (Dino Vournas)

reportedly resulted in over 90 percent of their achievements being applied to the armed forces' needs. Quantum communications research is just one area, with information grid networking and electromagnetic camouflage and protection also being researched.[30] The China Academy of Space Technology has done preparatory work to establish the country's first quantum remote-sensing laboratory. The aerospace community believes that remote sensing is an important area for the application of quantum information technology. It is hoped the laboratory will allow Institute 508 to apply for funding from the national 863 and 973 programs. Such a funding request appears appropriate because, in 2012, quantum information technology was designated as one of the four key areas of scientific research in the next 15 years.[31]

More recently, quantum communication received recognition as a key technology by the Chinese Academy of Sciences (CAS) after the university's president, Bai Chunli, announced plans to establish five innovation centers that would unite the country's leading scientists and experts in advanced science and technology. The fields of study were quantum information and technology, Tibet plateau and Earth system science, particle physics, brain science, and thorium molten salt reactors.[32] As a result, on January 15, 2014, China established the CAS Center for Excellence Quantum Information and Quantum Physics in Hefei. This new center is recognized as a model for the other four centers.[33]

Research, Academics, China's Education Dilemma, and Economic Impact

China considers itself second in the world in terms of research and development spending, and it has conducted original research in quantum communications that has had an international impact.[34] Research has been ongoing in CAS since 1998, when innovative projects along with quantum communications held interest.[35] Quantum topics have had high-level interest for some time. Former President Hu Jintao stated in a speech that quantum communications had exerted great influence on China's economic and social development.[36] Premier Wen Jiabao noted, "Quantum theory and the theory of relativity stimulated the development of semiconductors and microelectronic integrated circuit technology, information technology, laser technology, nuclear energy, and related technologies."[37] In 2011, Liu Yandong, state councilor and Communist Party of China Central Committee Political Bureau member, noted that quantum communications have made "fresh contributions to scientific development."[38] She stated in 2012 that quantum communication technology has important strategic significance in ensuring the safety of state information. More important, she made these remarks

while attending a ceremony to launch the financial information quantum communication verification network.[39]

With such high-level cover it is not surprising that China's rapid science and technology development has been tied to quantum information.[40] As an example of the use of quantum information, in 2011 CAS reported on cooperation between the Institute of Modern Physics and the International Atomic Energy Agency. The physics research team "reportedly made significant progress in the research on the quantum state of ion-atom collisions, contributing to the better understanding of plasma evolution and plasma state diagnosis."[41] Such discoveries are ongoing and expanding.[42]

China has been on a path to expand its overall technological capabilities. One approach has been to overhaul the country's education system. During China's Ninth Five-Year Plan (1996–2000), the government began to initiate actions to strengthen a number of higher learning and key disciplinary areas. The goal was to upgrade 100 institutions to greatly improve their quality of education, scientific research, management, and institutional efficiency. The select 100 institutions were expected to, through their own merit, easily "exert significant impact on the country's social and economic development, scientific and technological advancement, and the national defense."[43]

The availability of funding in China for basic research has also been increasing steadily. In 1986 the investment in basic research was only 80 million yuan (approximately $9 to $10 million).[44] By 2012, according to Chen Yiyu, director of the National Natural Science Foundation of China (NSFC), the Chinese government allocated more than 15 billion yuan ($2.38 billion) from the central budget to the NSFC. While only a portion of the money goes toward researching quantum information, the NSFC is a key source of funding for China's research and development on quantum properties and applications.

China's growing economy and increasing wealth make it easier than most other countries to sink money into research and development programs. During the U.S. Naval Research Laboratory's second annual Karles Invitational Conference, Zachary J. Lemnios, Assistant Secretary of Defense for Research and Engineering, pointed out that:

Nations with strong GDP growth—think China, Russia, South Korea—are using their increasing wealth to bolster investments in basic science, applied research, and advanced technology development, and these investments are increasingly focused. For example, the Chinese National Medium- to Long-Term Plan for the Development of Science and Technology (2005–2020), aims to make China an "indigenous innovator" by 2020, and to do this they are investing in 16 goal-oriented basic research "megaprojects," one of which is quantum research.[45]

Basic research is essential for innovation. While the United States spends more money overall in basic research than any other country, Chinese investments are rising at a faster rate. According to Dowling, "One of the things that concerns me in the United States right now is that we are falling behind in our investments, particularly in basic science research. . . . We are getting to the point where we are no longer even in the top ten in terms of per capita investment in basic research anymore."[46]

Despite its economic wealth, however, China still has a number of hurdles to overcome before it can become a global innovative force. Pan attributes some of China's lack of creativity to the high amount of pressure placed on students. Students devote years to intensive studying. However, according to Pan, they "are often incapable of developing independent solutions" due to a lack of creativity. There has been talk of changing the education system, but this has not yet happened. As Pan pointed out, there are simply too many students.[47]

China's academic and scientific efforts point to the country's desire to achieve global technical superiority. Williams, who recognizes that quantum technologies will likely one day offer tremendous benefits to society, also sees the importance of maintaining a competitive edge in research and development to maintain both innovative and economic superiority. According to Williams, "While quantum technologies clearly create a direct risk to national security, the bigger risk is the threat to economic security since a strong economy is required to drive a strong military and innovation and quantum technologies are likely to be an innovation driver for the 21st century."[48]

Physicist Paul Davies once wrote, "The nineteenth century was known as the machine age, the twentieth century will go down in history as the information age. I believe the twenty-first century will be the quantum age."[49] Quantum technology is still in its infancy. The first organization or government to achieve quantum communication or quantum computing will control the technology, giving that country an advantage in every respect.

Conclusion

According to a 2010 article published by *Time*, "China is now at the cutting-edge of military communications, transforming the field of cryptography and spotlighting a growing communications arms race."[50] China, intent on becoming a global technology innovative force, has been making huge strides in research and development in many areas including quantum communication. There is a major push in the country to become the frontrunner in breakthroughs that will one day lead to the first quantum computer and the perfect quantum communication network. Should China eventually win the race in achieving certain quantum-based technologies, it could have a significant impact on national security and China's role as an emerging superpower.

Quantum technologies have the potential to revolutionize secure communications for military and intelligence organizations. A quantum computer might one day be able to access information that had been archived but not yet declassified. Quantum technologies could also lead to revolutionary applications that might help propel a nation to economic superiority.

While China still lags behind developed nations in many ways, as its academic programs and research methodology continue to evolve, the country could eventually gain a lead in the research and development of quantum information. It is impossible to predict who will win the race for this revolutionary technology. However, one thing is certain: The force behind China's research and development programs is growing. **JFQ**

Notes

[1] Hiram M. Wolfe III, Raymond P. Schmidt, and Thomas N. Thompson, *Southeast Asia: Working Against the Tide, Part One* (Washington, DC: National Security Agency [NSA], June 1970), available at <www.nsa.gov/public_info/_files/cryptologic_histories/work_against_tide.pdf>. Released in 2004 by NSA in Freedom of Information Act Case # 41608.

[2] Ibid.

[3] Jonathan P. Dowling and Gerard J. Milburn, "Quantum Technology: The Second Quantum Revolution," *Philosophical Transactions A*, August 15, 2003, available at <http://arxiv.org/ftp/quant-ph/papers/0206/0206091.pdf>.

[4] Gregory Huang, "Master of Qubits," *New Scientist* 196, no. 2629 (November 10, 2007).

[5] "Key Laboratory of Quantum Information," School of Physical Sciences, University of Science and Technology of China Web site, available at <en.physics.ustc.edu.cn/research_9/Quantum/201107/t20110728_116550.html>.

[6] "Quantum Computer to Be Developed in 15 Years, Chinese Scientist Predicts," Xinhua, January 6, 2006, available at <http://english.peopledaily.com.cn/200601/06/eng20060106_233390.html>.

[7] Huang.

[8] Stefanie Schramm, "Pan's Dream," *Academics.com*, November 2, 2010, available at <www.academics.com/science/pan_s_dream_39586.html>.

[9] Ivan Deutsch, interview with author, November 13, 2012.

[10] "China Makes Breakthrough on Quantum Computer," *People's Daily*, February 7, 2013, available at <http://english.peopledaily.com.cn/202936/8126200.html>.

[11] Ibid.; one picosecond is the equivalent of one trillionth (10^-12) of a second.

[12] Ibid.

[13] Jonathan Dowling, telephone interview with author, September 7, 2012.

[14] Carl Williams, telephone interview with author, January 11, 2013.

[15] "China Successes in Test of Quantum Cryptography Network: Scientists," *People's Daily*, April 3, 2007, available at <http://english.peopledaily.com.cn/200704/03/eng20070403_363235.html>.

[16] "China Tests Secure Quantum Communication," Xinhua, November 29, 2005, available at <http://english.peopledaily.com.cn/200511/29/eng20051129_224358.html>.

[17] Williams.

[18] "Ten Most Significant Developments in Sci-Tech in 2006," *People's Daily*, January 22, 2007, available at <http://english.people.com.cn/200701/22/eng20070122_343621.html>.

[19] Stephen Chen, "Quantum Leap Claimed in Tighter Internet Security," *South China Morning Post* (Hong Kong), May 8, 2007.

[20] Chen Xia, "China Builds World's First Quantum Encrypted Gov't Network," *China.org.cn*, May 21, 2009, available at <www.china.org.cn/government/local_governments/2009-05/21/content_17813415.htm>.

[21] Alexandra Witze, "Quantum Teleportation Takes Leap: Two Teams Improve Long-Distance Information Transmission," *Science News* 181, no. 13 (June 30, 2012), 10.

[22] Juan Yin et al, "Quantum Teleportation and Entanglement Distribution Over 100-Kilometre Free-Space Channels," *Nature* 488 (August 9, 2012), 185.

[23] Cheng Yingqi, "Quantum of Solace as Breakthrough Looms," *China Daily*, October 17, 2013.

[24] Matthew Luce, "China's Secure Communications Quantum Leap," *China Brief* 10, no. 17, Jamestown Foundation, August 19, 2010, available at <www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=36772&cHash=104f9aac40>.

[25] Ibid.

[26] Discussions in this section developed in concert with Timothy Thomas.

[27] David McNally, "Army Researchers Seek Secure Quantum Communications," Army News Service, November 30, 2012.

[28] He Shuyuan et al., "Join Forces and Pool Wisdom to Forge National-Defense Equipment and Facilities…" *Jiafangjun Bao* [PLA Daily], July 26, 2011, available at <news.china.com.cn/rollnews/2011-07/26/content_9145749.htm>.

[29] Yang Zhijun, Yang Daichun, and Ma Shengwei, "PLA UST Promotes Integrated Development of Interdisciplinary Research," *Jiefangjun Bao* [PLA Daily], October 11, 2011.

[30] Yang Zhijun and Ma Shengwei, "PLA UST Promotes Cross-Disciplinary Fusion, Intensifies Military-Civilian Joint Endeavors—More than 740 Innovative Achievements Help Enhance Combat Capabilities of the Armed Forces," *Jiafangjun Bao* [PLA Daily], March 18, 2012, 1.

[31] *Zhongguo Hangtian Bao Online*, July 25, 2012.

[32] "China Establishes Advanced Science Research Centers," Xinhua, January 9, 2014.

[33] Zhu Lixin, "China's Top Quantum Tech Center Founded in Hefei," *China Daily*, January 15, 2014.

[34] Stephen Chen, "Science Chief Wants to See China Lead the Way in Scientific Breakthroughs," *South China Morning Post Online*, November 25, 2012, available at <www.scmp.com/news/china/article/1090163/science-chief-wants-see-china-lead-way-scientific-breakthroughs>.

[35] Wen Jiabao, "Actively Greeting the Dawn and the Challenges of New Science and Technology, *Xinhua Domestic Service*, July 2, 2012.

[36] "To Carry out in a Down-to-Earth Way the Strategy of Promoting Development Through Innovation—Third Commentary on Extensively Studying the Spirit of General Secretary Hu Jintao's Important Speech," *Jingji Ribao Online* (Chinese), July 31, 2012, available at <http://paper.ce.cn/jjrb/html/2012-07/31/content_125344.htm>.

[37] Summary of speech by Wen Jiabao, "Several Issues Regarding S&T," *Qiushi Online* 14 (Chinese), July 16, 2011, available at <www.gov.cn/ldhd/2011-07/16/content_1907593.htm>.

[38] Liu Yandong, "Striving to Break New Ground in Fundamental Research," *Qiushi Online* 15 (Chinese), August 1, 2011, available at <www.gov.cn/ldhd/2011-08/01/content_1917336.htm>.

[39] Discussions developed in concert with Timothy Thomas.

[40] Cheng Yingqi, "Tianjin Meeting a Hotbed of Scientific Exchange," *China Daily*, September 18, 2012, available at <www.chinadaily.com.cn/china/2012-09/18/content_15766622.htm>.

[41] Chinese Academy of Sciences, available at <http://english.cas.cn>.

[42] Discussions in the first two paragraphs of this section developed in concert with Timothy Thomas.

[43] "Project 211: A Brief Introduction," China Education and Research Network Web site, available at <www.edu.cn/20010101/21852.shtml>.

[44] Currency exchange rates for 1987 are not available. Calculation done based on 2002 rates. See "Central Gov't to Pour 2.4 Billion U.S. Dollars Into Sciences," Xinhua, March 27, 2012.

[45] Zachary J. Lemnios, "Introduction: Dr. Jerome Karle and Dr. Isabella Karle," speech during Second Annual Karles Invitational Conference, Department of Defense as Technology Incubators, August 27, 2012.

[46] Dowling.

[47] Schramm.

[48] Williams.

[49] Gerard J. Milburn, *Schrodinger's Machines: The Quantum Technology Reshaping Everyday Life* (New York: W.H. Freeman, 1997), preface.

[50] Christopher Shay, "China's Great Quantum Leap Forward," *Time*, September 9, 2010.

Students listen and take notes as General Dempsey speaks at Keystone course at National Defense University (DOD/Daniel Hinton)

Writing Faculty Papers for Joint Professional Military Education

By Thomas P. Galvin

In joint professional military education (JPME), there is no tool more powerful than the written word. Whether in the form of books, journal articles, opinion pieces, or course papers, students and faculty members demand high levels of intellectual rigor and reflection in both the products they read and the ones they produce. Scholarly writing requires precision in terminology and recognition of the limits and boundaries of one's arguments. When done well, written works make indelible and permanent contributions to our professional domain of knowledge.

One form of scholarly writing, faculty papers used as readings, plays an important role in JPME settings. The breadth of subjects that must be covered to satisfy the JPME requirements limits the ability to delve deeply into any one topic. Lesson material must be presented both effectively and efficiently. Sometimes this means that the best off-the-shelf readings (for example, journal articles, books, or book chapters) either are too long or detailed to be used, or else they present only a single side or perspective of a complex

Thomas P. Galvin is a Faculty Member in the Department of Command, Leadership, and Management at the U.S. Army War College. The author acknowledges Professor Charles D. Allen, U.S. Army War College, for his mentorship and comments on earlier drafts of this article.

issue. Faculty papers are useful tools to present synthesized literature reviews or illustrative examples that help bring disparate literature to life. In the assessment of the JPME faculty, these papers draw out the most relevant and practical aspects of an issue, which encourages dialogue among students.

It has been my experience that some JPME faculty, especially new faculty members, are less likely to engage in this kind of writing and more prone to rely on off-the-shelf readings even though the articles may not mesh well with the published lesson objectives. Although competing demands for time and comparative inexperience in academia are contributing factors to this phenomenon,[1] my purpose here is to address a factor that has received less attention. Just as the *Joint Force Quarterly* submissions page stresses that writing for publication is very different from preparing course papers,[2] developing high-quality lesson materials represents a wholly different form of scholarly writing. However, there is no how-to guide or blueprint available to help new JPME faculty members get past the hardest step—that is, getting started at converting one's expertise and interests into a faculty paper that others can use for teaching in seminar.

I posit that there are principles that explain why some faculty papers are used, revised, and reused year after year and why others are not. In this article, I offer three such principles that emerge from the more successful papers: theoretical grounding, bridging theory to practice, and proper use of illustrative examples. New faculty may find these principles helpful in organizing ideas, while seasoned faculty may find them useful for coaching and mentoring their professional colleagues.

Theoretical Grounding

Theoretical grounding is the process of using theory from appropriate disciplines (and from military or nonmilitary domains) to present the underlying ideas behind doctrine, processes, and so forth. This principle stems from the need to separate education from training. One common mistake made when writing lesson materials is to treat doctrine as though it were theory. Doctrine is an important result of theory but is not theory in itself. The educational value comes in understanding the dialogue and decisions that led to the doctrine, as it is the choices presented that future doctrine writers will face. The same can be said for regulations, processes, systems, tactics, techniques, and procedures that are often included in JPME courses. Theory provides a framework for getting past the *what* and to the *why*.

As many JPME lessons are focused on practice, the purpose of theoretical grounding is not necessarily to teach theory but rather to broaden practice and encourage dialogue on potential improvements or innovations. A review of a number of successful U.S. Army War College papers indicates that theoretical grounding can be accomplished in five ways.

By Explaining Complex Phenomena. The author chooses a key component or concept of a theory, uses it to explain a current phenomenon (such as a global situation or existing process), and then shows how it can be applied more generally. For example, the authors of a faculty paper on organizational culture chose components of several theories to explain dominant elements of U.S. Army culture.[3] Theoretical grounding demonstrated to students that the phenomenon of culture has been studied and is reasonably well understood, and accordingly it can be used to explain how the U.S. Army's culture formed and why it may be difficult to change. This explanation then leads to student dialogue on what influence leaders have over the Service culture.

By Presenting Tensions and Choices. The author chooses a theory that offers opportunities for students to make choices and see how those choices play out. Social science is replete with 2-by-2 matrices representing the interaction of two factors. An author armed with such a construct could use it to present the current state of doctrine, processes, systems, and so forth and to present options regarding how things could be different, enabling robust student dialogue on the implications. As an example, the aforementioned organizational culture paper presents Kim Cameron and Robert Quinn's competing values model to illustrate how the U.S. Army's scores on various organizational performance indicators illustrate not only its overall adherence to internal orientation and bureaucratic control but also its preferences for norms and values paradoxical to it. This helps engage students in dialogue on potential clashes of culture within the Army.[4]

By Elevating Students to Another Level. Some JPME, such as that provided by the war colleges, serves to bring students from one level of leadership to another (for example, from operational to strategic). Theory can serve as the basis for educating students on the similarities and differences. Lesson materials grounded in theory can help students break out of the familiar and embrace the new environment. An exemplar of such materials is the *Strategic Leadership Primer*, which comprises several faculty-written chapters, all well grounded in theory, that present the different tasks, competencies, and skills required of strategic leaders.[5] Some of the material is familiar to war college students who have already spent years as operational leaders, but the primer highlights how they may need to adapt their extant skills and competencies to the strategic environment they will enter after graduation.

By Distinguishing What Is Understood from What Is Not Well Understood. Theories do not explain everything; they have limitations and boundaries, and sometimes they conflict. The gaps can often be leveraged to discuss potential assumptions and biases held by students, catalyzing seminar dialogue. For example, one faculty paper on vision concludes by noting, "It should be clear that there is no 'cookie cutter' solution or best template for creating and implementing a vision."[6] This single sentence, which acknowledges the limits of what is known and understood *theoretically* about vision, offers students an opportunity to enter into rich and rewarding dialogue on what constitutes a "good enough" expression of vision using the concepts within the paper as a basis.

Student discussion in National War College seminar (NDU/Katherine Lewis)

By Clarifying Terms. Words have meaning, and too often they have multiple meanings, particularly in academia. Theoretical grounding includes the precise use of terms and levels of analysis. Good faculty papers help students navigate the meanings and uses, which is a useful skill to carry forward into practice. Two examples from the U.S. Army War College are short faculty papers on terms and principles concerning negotiation practices[7] and an overview of senior military officers' involvement in the Federal budgetary process.[8]

Bridging Theory to Practice

Sometimes finding the right fit between lesson objectives and readings is difficult, and this is particularly true regarding readings prepared by practitioners—opinion pieces and editorials, doctrine, regulations, government documents and reports, and studies by think tanks. JPME educators have to strike a balance between the requirements of the lesson, the availability of appropriate off-the-shelf readings, and the preparatory needs of the students (for example, reasonable reading load, sufficient time for reflection, and preparing for oral presentations when assigned). Sometimes the best answer is to develop a faculty paper that synthesizes the available material and encourages students to read further.

Building a strong bridge between theory and practice is critical because adult learners must be able to see the practical value of the theory being grounded. There should be clear signposts that the tensions and choices, gaps in knowledge and understanding, and so on present themselves in the source literature. The following three methods describe ways that faculty papers build this bridge.

By Addressing Practical Application to the Military Context. When theories are developed in nonmilitary contexts (such as management theories from business schools or macroeconomics), students may not fully appreciate their applicability to the military. Some may question the relevance, highlighting that the military is not like any other organization. While perhaps true, the similarities and differences between the military and other large complex organizations often influence how new ideas from society and business are introduced into the military and vice versa. Such ideas may not always be practical, but JPME should arm the students with well-reasoned arguments as to why not.

By Addressing "Hot" Topics. The cycle of publication in academic journals cannot always keep up with what is going on in the field.[9] The months (or years) between an author's final draft and publication are inadequate for satisfying the JPME requirement for presenting fresh and relevant educational materials. Faculty papers are well suited to address topics of current and heated debate and are easier to update with the latest information.

By Navigating and Filtering Difficult Theory. A clear indicator that a lesson is unsuccessful is when the students collectively demonstrate, through blank stares and dialogue that goes nowhere, that they did not "get it." Unquestionably, some theories (or the academic papers presenting them) are inherently difficult to read and understand. The translation of difficult concepts into plain language for practitioner use can often be best satisfied through a well-written faculty paper. Numerous past and current U.S. Army War College faculty papers, for example, serve this purpose. However, caution must be exercised to prevent concepts from being "dumbed down" or the introduction into the faculty paper of assumptions and biases disguised as part of the underpinning theory.

Proper Use of Illustrative Examples

Case studies, historical vignettes, and current events are popular ways of bringing theory and practice to life. They move the students from the abstract to the concrete, placing them in the shoes of military leaders facing difficult decisions related to the subject of the day. However, to be effective as educational tools, these examples have to reinforce the matters of theory and practice in the lesson. Off-the-shelf materials, such as published business cases or articles, may not always suffice. Best fit with the lesson is crucial.

Faculty papers that present such illustrative examples can either encompass the theory and practice or present only the example and refer back to theory and practice relayed in other readings. But coming up with the right examples is not easy, and sometimes the popular choice is not the best one for supporting the learning objectives. The most suitable readings are those that accomplish the following three tasks.

Illustrate Only Relevant Theory and Practice. Sometimes it is too easy to rely on a comprehensive off-the-shelf case study when a shorter, more targeted case is needed. Comprehensive cases can present digressions and distractions that pull students away from the subject. Exhibits and questions for dialogue should be drawn from the relevant theories and matters of practice, and the teacher's guide should provide instructions to faculty to help keep the dialogue focused appropriately.

Remain Consistent at the Right Level of Analysis. If the theory in question explains an organizational phenomenon (for example, culture), then the practice and examples should be written at the organizational level of analysis. If the theory regards an individual phenomenon (such as leadership), then the rest should be written at the individual level of analysis. If a subject involves multiple levels, the case must clearly navigate among them to avoid confusion.

Choose Either a Good Common Case or an Important Exception. Authors may choose a case based on their familiarity with it, which can sometimes be a mistake. Many JPME faculty members teaching the case may not be familiar with it and may suspect that a different case would be a better one to use. As the author chooses a case and prepares the teaching note, it may be useful to consider the following questions:

- Is this a good, suitable example that clearly illustrates the principles or tensions in the theory and matters of practice, such that the students can better achieve the lesson objectives?
- Is this a useful outlier of practical application that helps students better understand the breadth of issues explained by the theory?

Choosing a case applicable to the second question is tricky and occurs comparatively rarely given limited seminar time, but sometimes a contrasting example that exposes the limitations of theory and practice can be a powerful educational tool.

JPME faculty members enjoy a unique opportunity to quickly and markedly contribute to both student learning and the military's professional domain of expert knowledge through the production of quality faculty papers. Presenting ideas that stimulate dialogue and critical reflection is the goal. Also, student feedback helps faculty authors develop those ideas for pursuing publication. While there is no scientific formula or blueprint that guarantees a faculty paper will be reused for many years, the concepts of theoretical grounding, bridging theory to practice, and use of illustrative examples may help make their production more fruitful and generate useful contributions to both the JPME setting and the broader joint professional community. **JFQ**

Notes

[1] Joan Johnson-Freese, "The Reform of Military Education: Twenty-Five Years Later," *Orbis* 56, no. 1 (2012), 135–153.

[2] National Defense University Press, "JFQ Submission Guidelines and Writing Tips," available at <ndupress.ndu.edu/Home/SubmissionGuidelines.aspx>.

[3] Stephen J. Gerras, Leonard Wong, and Charles D. Allen, "Organizational Culture: Applying a Hybrid Model to the U.S. Army," U.S. Army War College faculty paper, 2008.

[4] Ibid., 3.

[5] Stephen J. Gerras, ed., *Strategic Leadership Primer*, 3rd ed. (Carlisle Barracks, PA: U.S. Army War College, 2010).

[6] Charles D. Allen and Andrew A. Hill, "Vision," U.S. Army War College faculty paper, 2012.

[7] George J. Woods, "Some Terminology and Definitions Used in 'Negotiating' Circles," U.S. Army War College faculty paper, 2007.

[8] Harold W. Lord, "Authorization or Appropriation," U.S. Army War College faculty paper, 2011.

[9] Jean M. Bartunek, "Academic-Practitioner Collaboration Need Not Require Joint or Relevant Research: Toward a Relational Scholarship of Integration," *Academy of Management Journal* 50, no. 6 (2007), 1323–1333.

Representative Ike Skelton, then Chairman of the House Armed Services Committee, begins hearing on Iraq, January 2007 (U.S. Air Force/D. Myles Cullen)

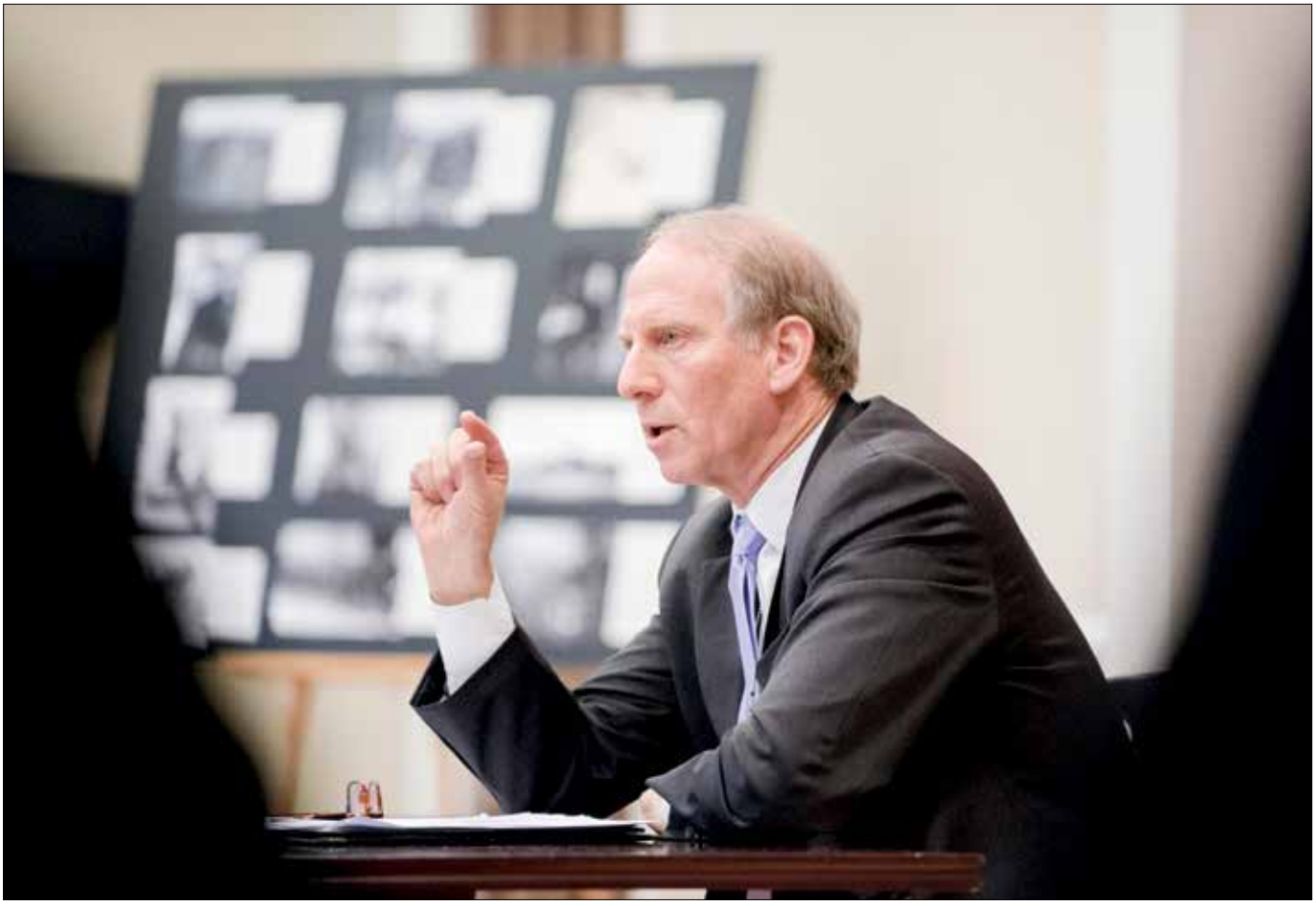
Joint Professional Military Education

A Retrospective of the Skelton Panel

By Anna T. Waggener

Unprecedented levels of joint Service cooperation occurred during the Iraq and Afghanistan wars. This teamwork did not come about by serendipity, but by the vision of the 1989 Report of the Panel on Military Education of the One Hundredth Congress (the Skelton Report) that described four elements within the joint professional military education (JPME) framework.[1] These elements would enhance the education of officers in each of the Services. Since that time, these elements have proved just as relevant today as they were more than 25 years ago. To ensure jointness, the Skelton Panel adopted several quantitative requirements. Each requirement, monitored by the Chairman of the Joint Chiefs of Staff, at JPME institutions builds the framework visualized by the Skelton Panel that promotes joint education to defend America

Dr. Anna T. Waggener was Director of Institutional Assessment at the U.S. Army War College.



American diplomat Richard Haass addresses senior military leadership during Strategic Studies Seminar at Eisenhower Executive Office Building in Washington, DC (DOD/Sean K. Harp)

against all threats today and well into the 21st century. To understand how best to use these requirements, we must understand what they are and how they contribute to joint acculturation.

At a time when the Nation faces threats across the globe, it is important to reflect on how JPME, envisioned by the Skelton Report, helps to ensure U.S. military officers are well prepared and developed to prevail against these threats.[2] Chairman of the Joint Chiefs of Staff Instruction 1800.01D (Change 1) of September 15, 2011, provides the requirements, standards, and learning areas to educate senior military and civilian leaders in strategy and policy to "produce the most professionally competent (strategic-minded, critical-thinking) individual possible."[3]

A watershed moment in joint officer education occurred when President Ronald Reagan signed the Goldwater-Nichols Department of Defense Reorganization Act of 1986, which designated the Chairman as the "principal military advisor to the president, National Security Council, and Secretary of Defense."[4] The full title of the Goldwater-Nichols Act is "A bill to amend title 10, United States Code, to strengthen the position of Chairman of the Joint Chiefs of Staff, to provide for more efficient and effective operation of the Armed Forces, and for other purposes."[5] As the title implies, accountability for ensuring jointness and education begins with the Chairman.

Three years later in 1989, then–House Armed Services Committee Chairman Les Aspin appointed then-Congressman Ike Skelton to lead a panel to conduct an assessment of military education. This panel developed the key recommendations that later became the requirements, standards, and learning areas set in the Chairman's policy for officer joint professional military education.[6]

The 1975 Department of Defense Committee on Excellence in Education, chaired by then–Deputy Secretary of Defense William Clements, influenced the 1989 Skelton Panel perspective with the concept that military education was to be "a broader and more balanced perspective."[7] With this in mind, the Skelton Panel adopted a framework that would build joint awareness, joint attitudes, and acculturation of the Services including civilians and international officers. The supporting structures to this broadened educational opportunity resulted in the rationale for four quantitative requirements as a way to ensure jointness: student-to-faculty ratio, military faculty mix, percentage of military instructors with specific previous education or experience, and class student mix.

Student-to-Faculty Ratio

The student-to-faculty ratio discussed in chapter V of the Skelton Panel report emerged as one of four quantitative requirements. The panel recommended "a relatively low student/faculty ratio overall ranging between 3 and 4 to 1, with the lower ratios at the senior schools"[8] that would give time for faculty to participate in traditional academic duties including research and service. The student-to-faculty ratio requirement for senior-level colleges not to exceed 3.5 students to 1 faculty member has not changed since it was set as a requirement by the Chairman in 1996. Difficulties in counting the respective faculty to include in the ratio have occurred over the years. Revisions in policy have attempted to define the counting process, yet joint education accreditation and reaffirmation program reviews have shown a wide variance in counting methodology. While civilian regional accrediting agencies provide detailed counting guidance, part of the counting difficulty in a joint education institution includes identifying faculty who are "full-time equivalents" among a mostly full-time faculty population. In its April 2010 report *Another Crossroads? Professional Military Education Two Decades After the Goldwater-Nichols Act and the Skelton Panel*, the House Armed Services Committee highlighted the difficulty in counting the ratio through the lens of accreditation reviews.[9] Afterward, the Deputy Director of the Joint Staff further explained counting faculty for the ratio in September 2010.[10] The outcome of this supplementing guidance was that the counting methodology narrowed the variance among JPME programs; the ratio more closely represented the actual number of faculty performing joint education instruction.

The envy of civilian colleges and universities, this low ratio of 3.5 students to 1 faculty member for senior-level colleges or 4 for intermediate-level colleges as an upper limit is not without controversy among joint education institutions. Endorsed by the Chairman's Joint Staff, the Military Education Coordination Council undertook a thorough examination of the ratio in 2012. The council concluded that the established student-to-faculty ratios "serve as single-point quantitative proxies for a host of harder to quantify characteristics of quality JPME institutions."[11] The result was to maintain the ratio based on possible increased faculty workload and possible decreased quality of education if the ratio were to be raised.[12]

Military Faculty Mix

The requirement for joint education institutions is to reflect a military faculty mix that is comprised of personnel from all the Services in the education process. This mix, defined in quantitative terms in policy, requires a split such as 60–40 percent or a proportional distribution, where the lesser percent represents nonhost military Services.

Most importantly, the lesser percent confirms the jointness of the teaching influences on the student learning experience, the main objective of the Skelton Panel. The senior-level colleges depend on nonhost military from other Services via a memorandum of agreement signed by the Service personnel chiefs and Deputy Chief of Staff of the Army for Army Operations, Plans, and Training to meet this requirement.[13] Nevertheless, there are difficulties or delays in providing the needed nonhost mix every year among some joint institutions due to force requirements.

Percentage of Military Instructors with Specific Previous Education or Experience

The same military faculty mix is subject to a required percentage of specific education and experience. The Skelton Panel recommended that military faculty possess credentials that apply to the level of education to which they are assigned to teach with "proven records of excellence and . . . a specific area expertise."[14] Policy translated this requirement into the quantitative measure that "seventy-five percent of the military faculty should be graduates of a senior-level PME program or be Joint Qualified Officers."[15] The same percent applies to intermediate-level PME programs with the added modification that they should be intermediate or senior-level graduates or Joint Qualified Officers.

Class Student Mix

Finally, the class and seminar mix is prescribed by policy in terms of expertise and Military Department, and like the military faculty mix, requires a split such as 60–40 percent, proportional distribution, or by a joint duty assignment list. Participating in a diverse, small group seminar of joint military, civilian, and international officers promotes the value of acculturation in the seminar. Bonds of friendship and understanding are formed during the shared educational experience that may prove critical in more than just military actions on the battlefield.

In his *2012 Army Strategic Planning Guidance*, General Raymond Odierno's "Prevent, Shape, Win" concept highlighted the possible outcomes of acculturation to win wars when he referred to the opportunities to establish relationships across the globe.[16] Civilian students representing various departments in the government enhance the education process, while learning about military culture for their own potential leadership positions. International officers from a variety of countries around the world provide other countries' perspectives and build relationships that may help prevent future conflicts with the United States. The Skelton Panel believed that "the objective of joint education should be to change officers' attitudes about developing and employing multi-service forces."[17]

Nonresident Education Programs

Joint education online programs (nonresident education programs), while not subject to the same quantitative measures described above, must be of the same high quality as education programs where students are in residence. These programs may employ combinations of residence and online learning, may accommodate each individual student or students as a group, and to the extent

possible, include a variety of Service mix, civilians, and international officers to promote jointness and acculturation.

In online programs, the four quantitative requirements of policy are met in a qualitative way that reflects the Chairman's intent. For example, student-to-faculty ratio is determined when comparing the delivery method to the needs of students. The military faculty mix and qualifications are demonstrated by representation of the Services, including the Reserve components. Diversity of class and student mix are evident when they include an assortment of all Services and interagency civilians to the maximum extent possible. At any rate, identifying the same characteristics in a qualitative way within an online program is an indicator that students are achieving the objectives of joint acculturation.

Common Educational Standards

Each institution and program, regardless if onsite resident education or nonresident education, intermediate-level college, or senior-level college, is accountable to the common educational standards (indicators that measure or describe academic excellence) defined in the Chairman's policy. The standards are similar to guidance or criteria in civilian regional accrediting agencies in that they address students, faculty, and resources in the broadest sense.[18] This education must promote joint awareness and be delivered using an effective instructional methodology focused on the adult learning model. The institution must also assess achievements of its students and overall effectiveness of the education program. Faculty members are recruited with appropriate academic credentials, assessed periodically, and participate in faculty development opportunities. Institutional resources must support the educational process.

Each program is qualitatively and quantitatively assessed in view of these standards during the onsite accreditation visit. Civilian regional accrediting agencies accredit the institution as a whole as they look at the educational processes and outcomes. On the other hand, the Process for Accreditation of Joint Education evaluation site visit considers each program as unique and reviews it compared to law and policy.[19] Both accrediting agencies, however, assist the institution and program in evaluating achievement of its mission, vision, goals, objectives, and strategic plans within the lens of its accreditation standards. The more each institution engages in the self-study process, the more it can improve student learning and achievement.

Joint Learning Areas and Learning Objectives

As prescribed by the Skelton Panel and later included in policy, joint institutions offer curricula based on prescribed learning areas appropriate to the level of education. For instance, unless an institution is specifically addressed in policy, senior-level colleges will study defined areas that include:

- National Security Strategy
- National Military Strategy
- Joint Warfare, Theater Strategy, and Campaigning in a Joint, Interagency, Intergovernmental, and Multinational Environment
- National and Joint Planning Systems and Processes
- Integration of Joint, Interagency, Intergovernmental, and Multinational Capabilities
- Joint Strategic Leadership.[20]

Subordinate learning objectives give more specific descriptions to the overall learning area. Courses are taught by both active and passive learning methods using readings with doctrinal emphasis, seminar dialogue, case studies and historical vignettes, lectures, and experiential learning opportunities that may span the entire program of study.

One of the requirements of the military onsite review for accreditation or reaffirmation of the program is to provide a mapping of each prescribed subordinate learning objective to each lesson taught. This matrix supports the evaluation site visit team in determining the extent to which the program meets the criteria of policy. The U.S. Army War College also maps learning areas to Bloom's Taxonomy levels of learning achievement to show the hierarchy of learning required on each topic.[21]

Peer Accreditation Reviews

Inherent with the responsibility of joint education review, the Chairman publishes the accreditation charter in policy. Similar to site visit teams for civilian regional accreditation evaluation, the teams prescribed by the Chairman's charter ensure the appropriate mix of peers based on key characteristics of the individuals to form an evaluation site team. Again, similar to civilian regional accreditation and reaffirmation, the program under review provides a self-study that describes how it meets the requirements in addition to standards and learning areas. The evaluation site team provides a review of findings that includes a recommendation to the Chairman regarding the status of accreditation at the end of the onsite evaluation visit.

Influences on Joint Education Policy

There are no doubts the National Defense Authorization Act of 2013 review of JPME research institutions and the study on overall joint military education processes will impact the next revision of the Chairman's policy.[22] In fact, in the October 2013 report to congressional committees, *Actions Needed to Implement DOD Recommendations for Enhancing Leadership Development*,[23] the Government Accountability Office accepted the Military Council's study on joint education and recommended setting timelines to implement the findings. Additionally, the Chairman's *Desired Leader Attributes for Joint Force 2020* will assist institutions in keeping joint learning areas and learning objectives aligned with his intent.[24] Other considerations certain to impact policy revision include a multitude of issues that have arisen since 2009, such as the military drawdown, constrained resources, online educational opportunities and student learning, knowledge management within an educational environment, and educational support technologies.

Conclusion

Of the four requirements to promote joint education—student-to-faculty ratio, military faculty mix, percentage of military faculty with specific previous education or experience, and class student mix—each measure is as important as the next. Combined with the specified learning areas and objectives, they build the framework visualized by the Skelton Panel that guides an officer throughout the remainder of a career and into the future. Dan McCauley's article "JPME: The Need for Foresight" offered a pointed observation when he combined policy with the Capstone Concept for Joint Operations. He repeated the call for "leaders capable of succeeding in fluid and perhaps chaotic operating environments" and compared this capability to the military's teaching on "nonlinearity, complexity, and uncertainty."[25]

These requirements, combined with the professional content and educational standards advanced by the Skelton Panel, build the framework for advancing the professional careers of the officer corps and the security of the Nation. JPME graduates meet the intent of the Chairman's vision to ensure "that officers are properly prepared for their leadership roles at every level of activity and employment, and through this, ensure that the U.S. Armed Forces remain capable of defeating today's threat and tomorrow's."[26] Strategy and policy will continue to adapt and change. The current drawdown and a possible follow-on sequester will make sustaining the current level of jointness more difficult to some degree. While we welcome the end of two significant military engagements, the return to a garrisoned force comes at the risk of a return to Service-oriented forces. In short, both the four elements and the spirit advanced by the Skelton Panel have served JPME and the joint force well. We need to sustain these elements and for good reasons. Joint education is the foundation upon which our national and military security strategies are learned, understood, and initiated. To guarantee that our military stands ready to defend America against all threats and challenges, we need to retain the cultural advancements initiated by the Skelton Panel more than 25 years ago. **JFQ**

Notes

[1] U.S. Congress, House of Representatives, Committee on Armed Services, *Report of the Panel on Military Education of the One Hundredth Congress*, 101st Cong., 1st sess., 1989, no. 4, available at <http://catalog.hathitrust.org/Record/007602201>. Hereafter, the Skelton Report.

[2] Chairman of the Joint Chiefs of Staff (CJCS) Instruction 1800.01D (CH 1), "Officer Professional Military Education Policy (OPMEP)," September 15, 2011, available at <http://dtic.mil/doctrine/education/officer_JPME/cjcsi1800_01d.pdf>.

[3] Ibid., A-1.

[4] H.R. 3622, Goldwater-Nichols Department of Defense Reorganization Act of 1986.

[5] Ibid.

[6] Skelton Report.

[7] Richard L. Davis and Frank P. Donnini, eds., *Professional Military Education for Air Force Officers: Comments and Criticisms*, Defense Technical Information Center, 9, available at <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA421950>.

[8] Skelton Report, 143.

[9] House Committee on Armed Services, Subcommittee on Oversight and Investigations, *Another Crossroads? Professional Military Education Two Decades After the Goldwater-Nichols Act and the Skelton Panel*, H.R. 111-4 (Washington, DC: House Committee on Armed Services, April 2010), 121, available at <http://democrats.armedservices.house.gov/index.cfm/files/serve?File_id=d4748d4a-b358-49d7-8c9a-aa0ba6f581a6>.

[10] "The Joint Staff Memorandum for PAJE Team Members, Subject: Standing Operating Procedures (SOP) for Counting Faculty and Student Ratios during Process for Accreditation of Joint Education (PAJE) Assessments," September 8, 2010.

[11] Military Education Coordination Council Working Group, *Rationale for OPMEP Student-to-Faculty Ratio Standards for Joint Professional Military Education*, Student-to-Faculty Ratio Study–Final Report, February 8, 2012.

[12] Ibid.

[13] "Memorandum of Agreement: Assignment of Military Faculty at Service Senior Level Colleges," signed December 30, 2005, by Deputy Chief of Staff G-3/5/7 (U.S. Army), Deputy Chief of Naval Operations (U.S. Navy), Deputy Chief of Staff Personnel (U.S. Air Force), and Deputy Commandant, Manpower and Reserve Affairs (U.S. Marine Corps).

[14] Skelton Report, 3.

[15] CJCS Instruction 1800.01D (CH 1).

[16] *2012 Army Strategic Planning Guidance* (Washington, DC: Headquarters Department of the Army, 2012), available at <http://usarmy.vo.llnwd.net/e2/c/downloads/243816.pdf>.

[17] Skelton Report, 57.

[18] Middle States Commission of Colleges and Schools, New England Association of Schools and Colleges, North Central Association of Colleges and Schools, Northwest Commission on Colleges and Universities, Southern Association of Colleges and Schools, and Western Association of Schools and Colleges.

[19] CJCS Instruction 1800.01D (CH 1).

[20] Ibid., "Service Senior-Level Colleges Joint Learning Areas and Objectives (JPME Phase II)," E-E-1.

[21] Ibid., "Bloom's Taxonomy, the Cognitive Domain: Evaluation, Synthesis, Analysis, Application, Comprehension, and Knowledge," E-A-1.

[22] Leon E. Panetta, *Review of Joint Professional Military Education Research Institutions* (351808), February 19, 2013, and *Joint Professional Military Education* (351810), February 20, 2013.

[23] U.S. Government Accountability Office, *Actions Needed to Implement DOD Recommendations for Enhancing Leadership Development*, Report to Congressional Committees, Joint Military Education, GAO-14-29, October 2013, available at <www.gao.gov/assets/660/658527.pdf>.

[24] Chairman of the Joint Chiefs of Staff, *Joint Education White Paper* (Washington, DC: The Joint Staff, July 16, 2012), available at <http://www.jcs.mil/content/files/2012-07/071812110954_CJCS_Joint_Education_White_Paper.pdf>.

[25] Dan McCauley, "JPME: The Need for Foresight," *Small Wars Journal*, May 24, 2013, available at <http://smallwarsjournal.com/jrnl/art/jpme-the-need-for-foresight>.

[26] CJCS Instruction 1800.01D (CH 1).

U.S. Army General Matthew Ridgway (second from left) in Ribera, Sicily, July 25, 1943

On Operational Leadership

By Milan Vego

There were commanders-in-chiefs who could not have led a cavalry regiment with distinction and cavalry commanders who could have led armies.

—Carl von Clausewitz

Success of any military organization depends on the experience and good judgment of its leaders. Ideally, all commanders should have a high level of professional education and training in addition to some critically important character traits. Moreover, the higher the level of command, the more important it is that commanders and staff meet these requirements. Wars are not won or lost at the tactical level but at the operational and strategic levels. Hence, it is critically important that operational commanders are selected based solely on their proven or potential warfighting abilities and not their political connections or manage-

Dr. Milan Vego is R.K. Turner Professor of Operational Art in the Joint Military Operations Department at the Naval War College.

ment skills. Operational commanders are not managers but should be first and foremost warfighters.

Leadership vs. Management

Leadership can be defined as the art of influencing others and environments directly and indirectly and the skill of creating conditions for sustained organizational success to achieve desired results.[1] The quality of one's leadership cannot be quantified in any meaningful way. It is essentially intangible. Leadership and management are not identical things. Management deals with the allocation and control of resources—whether human, material, or financial—to attain the objectives of an organization.[2] Traditionally, superiority in materiel was one reason that the U.S. military emphasized management thinking and a business approach to solving military problems. Among other things, the strong emphasis on the managerial values and entrepreneurial ethics contributed significantly to the inability of the U.S. Army to perform well during the Vietnam War.[3]

Despite these negative experiences, the U.S. military apparently did not learn the proper lessons; a business approach to the conduct to war is alive and well in the U.S. military. An emphasis is still put on management and military efficiency instead of effectiveness. Various quantifiable methods called "metrics," based on business models, are extensively used to evaluate the performance of U.S. forces in combat. But experience shows that one's military performance is bound to be dismal against a strong and skillful opponent unless there is a consistent and strong emphasis on leadership and warfighting in peacetime. Also, the conduct of war is largely an art and not a science or akin to a business activity.

The Term

In generic terms, *operational leadership* refers to those commanders and their staffs who need to think operationally instead of tactically in exercising their authority and responsibilities across the entire spectrum of conflict—that is, from peacetime competition to operations short of war and high-intensity conventional war. They range from an army corps and its naval/air equivalents (numbered fleets/air forces) to the theater armies/fleets/air forces and multi-Service (joint) theater commands (theater of war/theater of operations). Theater commands are the principal operational levels of command because they have sufficient forces to conduct campaigns/major operations. The lowest level of command that could plan and execute a major operation is the joint/combined task forces and in some cases even single divisions (as Operation *Iraqi Freedom* in 2003 illustrated).

Personality Traits

Successful operational commanders usually do not have some inborn qualities that set them apart from successful tactical commanders. Both operational and tactical commanders need to possess a good balance of the most important personality traits. In contrast to a tactical commander, the personality and command style of an operational commander is understood indirectly rather than directly through the chain of command. This is especially true in the case of naval or air operational commanders because their subordinate forces are deployed over a large part of a theater. Another major difference is that an operational commander cannot be successful without thinking operationally versus tactically in performing his numerous responsibilities in peacetime and in time of war.

Personality traits of commanders at any echelon include strong character, personal integrity, high intellect, sound judgment, courage, boldness, creativity, presence of mind, healthy ambition, humility, mental flexibility, foresight, mental agility, decisiveness, understanding of human nature, and the ability to communicate ideas clearly and succinctly. Clearly, no commander can ever have all these traits represented in equal measure. Perhaps the most critical of these for success are a strong character, high intellect, creativity, and boldness. These qualities are developed throughout life and a military career—and through self-study.[4]

Operational Thinking

One of the principal requirements for success at the operational and strategic levels of command is to think broadly and have a broad vision.[5] Such ability, which Germans call *operatives Denken* (operational thinking), is only in some rare cases the result of a commander's inherent predisposition to think big and far ahead of current events. Operational thinking is not identical to what information warfare advocates call "situational awareness" (SA).[6] The extensive use of this term in the U.S. and other militaries is one of the best proofs of tactical vs. operational thinking therein.

Many classical military thinkers and practitioners of warfare have recognized the need for commanders to think in broad terms. Prussian General Gerhard Johann David von Scharnhorst (1755–1813), for example, observed, "One has to see the whole before seeing its parts. This is really the first rule, and its correctness can be learned from a study of history."[7] Field Marshal Helmuth von Moltke, Sr. (1800–1891), wrote, "All individual successes achieved through the courage of our [German] troops on the battlefield are useless if not guided by great thoughts and directed by the purpose of the campaign and the war as a whole."[8] He believed that "it is far more important that the high commander retain a clear perspective of the entire state of affairs than that any detail is carried out in a particular way."[9] Moltke, Sr., also wrote, "All successive acts of war are thus not premeditated implementations of some plan but spontaneous actions in response to the military situation of the moment. What is important, in each concrete case, is to see clearly through a mist of uncertainty, assess the facts accurately, guess the unknowns, reach a decision quickly, and then move to carry it out vigorously without letting oneself be sidetracked."[10]

Importance

An operational commander should think operationally in exercising his

Lieutenant General George S. Patton, U.S. Third Army commander, pins Silver Star on Private Ernest A. Jenkins of New York City (NARA)

responsibilities and authority across the entire spectrum of conflict. Obviously, operational thinking is the most critically important in a high-intensity conventional war. Yet all types of operations short of war, such as combating maritime terrorism/piracy, counterinsurgency, and peace operations, also require that operational commanders think operationally rather than tactically.

Operational thinking helps the commander to employ friendly forces in such a way that each action directly or indirectly contributes to the accomplishment of the ultimate strategic or operational objective. Hence, an operational commander must have the ability to build a strategic or operational "picture" of the situation in a theater. This means an uncanny ability to know and understand all military and nonmilitary aspects of the situation in a theater, reduce complexities of the situation to their essentials by properly differentiating between important and less important or trivial elements, link disparate events ("connect the dots"), deduce patterns, and envisage future trends in the situation for several weeks or even months. The operational commander who does not think operationally may eventually be successful but at substantially heavier costs for friendly forces in terms of personnel, materiel, and time than the commander who skillfully applies the tenets of operational leadership. Moreover, there is always a great risk that a weaker opponent who thinks operationally could inflict large losses on, or even defeat, larger but poorly led forces.

Operational thinking is both a foundation and framework for developing *operational vision*—that is, the commander's ability to envisage correctly the flow of events until the ultimate objective of a major operation or campaign is accomplished. This means the commander has to think like a good chess player in terms of combination (action-reaction-counterreaction) until the military endstate is achieved. As in a game of chess, the operational commander who views the board as a single interrelated plane of action and each move as a prelude to a series of further moves is more likely to be successful than an opponent who thinks only a single move at a time. Operational commanders should think of how to create opportunities for the employment of their forces while at the same time reducing the enemy's future options.[11]

By correctly anticipating the enemy's reaction to his own actions, the operational commander can timely make a sound decision, act, and then prepare to make another decision to respond to the enemy's reaction. The key to success is to operate within the enemy's decision cycle. Without this ability, the operational commander cannot seize and maintain initiative, and without this initiative, his freedom of action is greatly restricted by the opponent.

Operational vision is inherently narrower in its scope than operational thinking, and in terms of time is limited to anticipated duration of a campaign/major operation. No campaign or major operation can be coherently planned and executed without a vision of how it should end. Among other things, operational vision ensures that an operational commander is focused on defeating or neutralizing the enemy center of gravity instead of being distracted by the pursuit of purely geographic or economic objectives. Practical application of operational

vision is in formulating and articulating *operational commander's intent.*

History gives many examples of highly successful operational commanders. Perhaps with few exceptions, most of them were both thinkers and practitioners of operational art; there is no contradiction between the two. Napoleon I (1769–1821), Moltke, Sr., and Field Marshal Erich von Manstein (1887–1973) belong to a small, select group of brilliant operational thinkers and practitioners. There is also a relatively large group of above average to excellent operational commanders of all three services who conducted successful campaigns and major operations, such as Field Marshals Albert Kesselring, Erwin Rommel, and William S. Slim; Marshal Georgy Zhukov; Generals Douglas MacArthur, George S. Patton, Bernard L. Montgomery, and George T. Kenney; and Admirals Ernest J. King, Chester W. Nimitz, Raymond A. Spruance, Andrew Cunningham, Erich Raeder, and Karl Doenitz. Since the end of World War II, there have been only a few operational commanders who performed excellently in combat. Perhaps one of the best but most underappreciated U.S. military leaders in the postwar era was General Matthew B. Ridgway. He performed superbly as the U.S. 8th Army commander by turning the situation around in Korea in the spring of 1951.[12]

The inability to think operationally has resulted in major setbacks or even failures of campaigns or major operations. For example, the lack of operational thinking was the main reason for the Allied defeats in Norway and France in 1940 and in Southeast Asia in 1941–1942. Besides the serious disconnect at the U.S. strategy and policy level, the Vietnam War was essentially conducted at the theater-strategic and tactical levels only; again, operational art was not applied.[13] A major reason for the Argentine defeat in the Falklands/Malvinas War of 1982 was the lack of operational thinking. Likewise, the Iraq-Iran War (1980–1988) degenerated into a war of attrition at the operational level because of the lack of operational thinking by both sides.

Attributes

Operational thinking encompasses several critical and diverse but closely related attributes. The most important for the commander are having an operational rather than a tactical perspective; balancing operational factors with the objective; fully understanding the levels of war and their interrelationships; understanding geography and operational features of the operating environment; making sound operational decisions; and fully comprehending the linkage among policy and strategy, operational art, and tactics.

Perhaps the most important proof of operational thinking is the commander's ability to have an *operational* instead of *tactical* perspective. In terms of the factor space, the operational commander's area of responsibility is a theater or major part of it. The size of a theater can vary from several hundred to millions of square miles. For example, U.S. Pacific Command encompasses an area of about 100 million square miles with 44 countries, while U.S. Central Command encompasses an area of about 21 million square miles with 51 countries. In contrast, the perspective of a tactical commander is much smaller because it pertains to a given combat zone/sector or area of responsibility. In terms of time, an operational commander has to assess a situation several weeks or even months ahead, while the time window for a tactical commander is from several hours to 2 or 3 days.

An operational commander should evaluate fully the influence of nonmilitary aspects of the situation (political, diplomatic, economic, religious, legal, environmental, informational, and others) on planning and employing forces. This requirement is not something entirely new as some leading proponents of information warfare falsely claim. For example, Frederick the Great pointed out that policy and military art must be taken into account in preparing for a campaign.[14] He wrote that one should "know one's enemies, their alliances, their resources, and the nature of their country in order to plan a campaign. One should know what to expect of one's friends, what resources one has oneself and see the future effects to determine what one has to fear or hope from political maneuvers."[15] Moltke, Sr., was the first German chief of the general staff to demand that military-political considerations be included in operational planning. He invariably based his plans on the advantages and disadvantages of the military-political situation.[16]

Needless to say, an operational commander should have a thorough knowledge and understanding of the theory and practice of operational art.[17] Otherwise, he will not be able to have an operational perspective in assessing the situation in his theater and then to make sound decisions. At the same time, an operational commander must have solid knowledge and understanding of tactics in his chosen specialty and tactics of other combat arms/branches of his service. He also needs to have a full understanding of the tactical employment of forces of other services.

Another major problem is applying a "targeteering" approach to warfare—that is, when the focus of planning is on targets to be degraded, neutralized, or destroyed. It is also common to determine targets first and only then formulate objectives. In U.S. practice, many commands and agencies, from the Joint Staff to tactical commanders in the field, are involved in target development, selection, and approval.

Moreover, an operational commander will lose operational perspective if he grossly interferes with the responsibilities of his subordinate tactical commanders. By "micromanaging" subordinate commanders, an operational commander would spend time and effort on the things that would be better left to the commanders on the scene of action. This unwillingness to delegate authority is often the result of the so-called zero-defect tolerance or when the higher commanders do not tolerate mistakes made by subordinates. The end result of such a style of command is waiting on orders, lack of motivation, stifling creativity, and careerism on the part of subordinates. This cannot but have highly negative consequences on performance in combat. Another

Brigadier General Courtney Whitney, General Douglas MacArthur, and Major General Edward M. Almond observe shelling of Inchon from USS *Mt. McKinley*, September 15, 1950 (NARA/U.S. Army/Nutter)

problem is the false belief that advanced information technologies allow better assessment of situations by an operational commander than his subordinate tactical commanders. Frequent interference of an operational commander with the responsibilities of tactical commanders is the best proof that the operational commander does not trust subordinate ability to exercise initiative based on commander's intent. Moltke, Sr., stated that the most unfortunate of all high commanders is the one who is under close supervision and who has to give an account of his plans and intentions every hour of every day. This supervision may be exercised through a delegate of the highest authority at the headquarters or a telegraph wire attached to his back. In such cases, all independence, quick decisions, and audacious risk, without which no war can be conducted, are sacrificed. An audacious decision can be arrived at by one man only.[18] An operational commander's freedom of action is achieved primarily by properly balancing the factors of space, time, and force with a selected operational/strategic objective.[19] These operational factors and, increasingly, information are critically important to make sound decisions. This means among other things that a deficiency or disadvantage in one factor or element must be roughly balanced by surpluses or advantages in others. Bringing these factors into harmony with an objective requires a thorough knowledge and understanding of all the military and nonmilitary aspects of the situation. Any serious imbalance could be among other things resolved by scaling down the size of the objective or reducing the factor of space or increasing the factor time or force. Balancing of the operational factors versus the objective is largely an art rather than a science. The most successful operational commanders consistently displayed a high ability to harmonize the factors of space, time, and forces against the objective in planning and executing their campaigns and major operations.

Operational warfare is largely war on a map. Almost all successful operational commanders have had a solid knowledge of geography and a good appreciation of the operational features of the physical environment. Napoleon I was once asked how he always divined the intentions of the enemy so accurately. He responded, "I did not know beforehand the mistakes the enemy would make which I took advantage of; I simply studied my map." Napoleon I continuously studied the

enemy's possibilities and limitations on the map, much more than the enemy did. Yet the methods that brought Napoleon I his many successes in central Europe failed him altogether in Russia in 1812. In that instance, he failed to properly evaluate the factors of space and time versus the strategic objective. Rommel was known for his excellent knowledge of terrain and orientation.[20] MacArthur was also well known for his excellent knowledge of military geography, which greatly helped him to evaluate the factors of space, time, and force in planning and executing campaigns and major operations.

Operational commanders must fully understand the distinctions among three main levels of war (strategic, operational, and tactical) and how decisions and actions at one level affect events at the others. Among other things, a comprehensive understanding of the levels of war and their mutual relationships is the key prerequisite for operational commanders and their staffs in sequencing and synchronizing the use of military and nonmilitary sources of power in accomplishing strategic or operational objectives. Each level of war is directly related to the corresponding military objective to be accomplished. Hence, tactical, operational, and strategic levels of war are differentiated. Moreover, military objectives determine methods of combat employment of one's forces (tactical actions, major operations, campaigns) and therefore the size of the area in which opposing combat forces would operate. The operational level of war exists when a single military- or theater-strategic objective has to be accomplished as in Iraq in 2003. The higher the level of war, the more complex the situation military commanders and their staffs must understand, evaluate, and synthesize. Both military and nonmilitary aspects of situations are critical for success at the operational and strategic levels of war across the spectrum of conflict. This is not necessarily the case at the tactical level, except in the posthostilities phase of a campaign or operations other than war.

Although related, levels of war and levels of command are not identical. The levels of war exist only in time of open hostilities. In contrast, levels of command exist in time of peace and war. They are only prerequisites for conducting war at a given level in the course of accomplishing assigned military objectives. Yet if the respective theater commander does not apply the tenets of operational art in the use of his sources of power and instead focuses on tactics or, even worse, pure targeteering, he does not conduct war at the operational or theater-strategic level.

The highest art of operational leadership is making timely and sound decisions. The principal factors in decisionmaking should be the *mission* and *situation*. Among other things, the decision is a reflection of the personality traits, professional knowledge, and experience of the commander. In general, the higher the command level, the fewer but more important decisions are made—and more time is available to make these decisions. The much larger perspective at the operational level of command requires a more complex and challenging decisionmaking process than at the tactical level. A campaign or major operation is conducted over a much larger part of the theater and involves considerably larger and more diverse forces than tactical actions. The operational commander needs to evaluate the situation in all its complexity for several weeks or even months ahead. Often the operational commander must make decisions without having all the information available.[21] Despite significant advances in technology, the information available is usually ambiguous, incomplete, or outright contradictory. It also often arrives late. In combat it is common to have incomplete knowledge of the situation. Hence, an operational commander must make many decisions based on assumptions that might be partially or even completely false.

An operational commander cannot be highly successful without having full knowledge and understanding of the mutual interrelationships and linkage between strategy on one hand and strategy, operational art, and tactics on the other. All three components of military art are closely related. Strategy dominates operational art, and the latter in turn dominates tactics. Actions and events at the tactical level often affect strategy and policy in profound ways. Operational art is a critical link between strategy and tactics, and if that connection is weak or broken, no favorable strategic results can be achieved quickly or decisively. Whenever the ends and means at the national-strategic level are seriously disconnected or mismatched, brilliance at the operational and tactical levels—as the Germans consistently displayed during World War II—can only delay, but cannot ultimately prevent, defeat at the strategic level of war.

Obtaining Operational Thinking

The commander's ability to think operationally is a result of the influences of many factors. The societal and cultural framework determines to a large degree the nature of military institutions and hence professional education and training. Among other things, the commander's operational thinking is a product of the national way of warfare as a whole and the common operational outlook of the armed forces or a particular service. Sound joint doctrine and training are the main tools for acquiring a common operational outlook.

The most important direct influence in shaping the future operational commander's ability to think broadly is participation in field trips, planning/war games, large-scale exercises and maneuvers, and commanding large forces. Obviously, the most important of all direct influences is combat experience. However, most future operational commanders rarely have the opportunity to take part in combat. Hence, the best way to obtain operational thinking is to attend service/joint war colleges, preferably their resident programs. Another method is self-education. Officers should make continuous efforts to improve their professional knowledge over the entire length of their military career. The better educated the commander, the more he understands the big picture and the better he will perform (provided the commander has the essential qualities of character).[22] All great captains in history, such as Julius Caesar (100–44 BCE), Gustavus Adolphus

of Sweden (1594–1632), Henri de la Tour d'Auvergne, Viscomte de Turenne (1611–1675), Napoleon I, and Moltke, Sr., constantly worked to improve their professional knowledge. Napoleon I was known for untiring study and never failed to avail himself of an opportunity to perfect himself.[23] Moltke, Sr., was extremely well read in all aspects of the military profession.[24]

The critical study of past wars, and campaigns and major operations in particular, is a major source for developing the operational perspective of future commanders. Because few military commanders have experience commanding forces at the operational level, the best way to educate them to think operationally is through the study of the successes and failures of great military leaders. Some of the greatest military leaders were also great students of history. Operational commanders should be students of history, not historians (a big difference exists between the two).

Future operational commanders should have a broad knowledge of foreign policy, diplomacy, geopolitics, international economy, finance, ethnicities, religions, and other issues that shape the situation in any given theater. They need to have a thorough knowledge of the area in which their forces will be employed. They should also have a deep knowledge of other countries' histories, societies, and cultures.

Tenets

Success in combat is considerably enhanced when the operational commander applies certain tenets of operational art. These tenets are related but not necessarily identical to the principles of war. Perhaps the most important tenets of operational leadership are firm and unwavering focus on the objective, obtaining/maintaining freedom of action, exercising initiative, taking high but prudent risks, and applying overwhelming power at a decisive place and time.

The single most important element of operational art is accomplishing the military objective at hand. In addition to the levels of war, methods of combat employment of one's forces (tactical actions, major operations, campaigns) and their elements (for example, center of gravity, maneuver, deception, point of culmination) are directly or indirectly related to the scale of the objective. Thus, one of the most important tenets of operational leadership is to have a firm and unwavering focus on accomplishing the *ultimate objective* of a campaign or major operation. The objective, once selected, must be adhered to. However, the initially selected objective should be changed, modified, or even abandoned as demanded by the changes in the situation. The operational commander should realize that there is always more than one way to accomplish that objective.[25] There is probably no greater mistake than to determine and pursue several operational/strategic objectives simultaneously. Such a course of action can be taken only if one's forces possess overwhelming power against any conceivable combination of enemy forces. Any effort to weaken the importance of a military objective, as the proponents of effects-based operations have done, is the antithesis of operational thinking and practice.

Also important is the commander's ability to *obtain and maintain freedom of action*—that is, to act effectively at any time in meeting threats.[26] The operational commander should always try to obtain and maintain freedom of action.[27] Otherwise, his ability to exercise the initiative is lost.[28] The operational commander should also do everything possible to reduce the enemy's freedom to act.[29] In practice, freedom of action for an operational commander is invariably subject to certain political, diplomatic, military, economic, social, legal, and, today, environmental limitations. In general, the more limitations on the operational commander's freedom of action, the fewer the means and ways the political leadership will have for accomplishing its stated political strategic objectives.[30]

Freedom to act is an absolute prerequisite for exercising the *initiative* on the part of subordinate commanders. The more freedom of action given to subordinate commanders, the more room they have to exercise initiative. To ensure sufficient freedom for subordinate commanders, an operational commander should apply the German-style mission command (*Auftragstaktik*). In general, this method of command and control allows greater flexibility than centralized command and control for adapting rapidly to changing battlefield situations, dealing with unforeseen problems, and exploiting fleeting opportunities.[31] Moltke, Sr., emphasized that the advantage of a situation would never be fully used if subordinate commanders waited for orders. Only if the commanders at all levels were competent for and accustomed to independent action would the possibility exist for moving large masses with ease.[32] A higher commander provides only those details necessary for understanding and coordinating and leaves a lot of room for independent action for subordinate commanders in accomplishing the assigned missions.[33] The main prerequisites for the successful application of mission command were the commander's proper understanding of the nature of war, common operational or tactical outlook, sound doctrine, excellent leadership, a high level of professional education and training, and common vocabulary.

The mission command method of command and control is most suited to a fast-moving and changing situation on the battlefield, as is in a high-intensity conventional war. It is a loose, decentralized method of command and control predicated on an understanding of overall mission requirements rather than on compliance with detailed direction from above. In general, it allows greater flexibility than centralized command and control for adapting rapidly to changing battlefield situations, dealing with unforeseen problems, and exploiting fleeting opportunities.[34] The single most important advantage of mission command is that it encourages creativity and initiative on the part of subordinates. It requires steady emphasis on leadership and warfighting at all levels of command. It also greatly enhances the role and value of professional education and training among officers and the rank and file. A major shortcoming of mission command

Iranian journalists jump from helicopter in West Front of Iran-Iraq War (Courtesy SAJED)

is that a subordinate commander may sometimes cause an unwanted escalation or worsening of the situation. In addition, lower decisionmaking thresholds and highly diffuse centers of authority can make coordination among command elements more difficult, thereby increasing the risk of loss of control by the commander. Another pitfall in applying mission command is incompetence in subordinate commanders. The successful application of mission command is also compounded when operational commanders interfere in purely tactical decisions and actions.[35] Risk aversion and zero-defect tolerance so prevalent in the U.S. and other Western militaries are the antithesis of the German-style mission command.

In general, mission command cannot be applied fully or at all when there is a need for an urgent action or where the highest leadership cannot afford an error that can easily lead to severe political or strategic consequences. Examples of such situations today are in conflict prevention/management, posthostilities, and peace operations. The principal elements of mission command are the mission, situation, commander's intent, freedom to act, and initiative. These elements have to be skillfully applied by both the higher and subordinate commanders.

Commander's intent is the principal tool in ensuring freedom of action for subordinate commanders. In the German military prior to 1945, commander's intent was sacrosanct. The intent provided a framework within which an isolated subordinate commander could act in the spirit of the mission issued by a higher commander.[36] It promoted unity of effort in a fluid situation that failed to conform precisely to one's plans and expectations. The intent was aimed both to circumscribe and encourage subordinate commanders' exercise of the initiative.[37] The execution of the mission in accordance with the higher commander's intent required not only independence and ability of analysis, but also what the Germans called "thinking obedience" (*denkende Gehorsam*). The Germans put great importance on the need to maintain the initiative once it was obtained.[38] Moltke, Sr., fostered critical thinking and independent actions among his subordinates. He believed that the best results are achieved when a commander acts within the framework of his higher commander's intent.[39]

The higher the command echelon, the larger the area of uncertainty, and the higher the risks the commander should take. Despite all the advances in information technologies, there will always be a rather large area of uncertainty in any given operational or strategic situation. Among other things, the operational commander rarely, if ever, has complete knowledge of all the factors in a situation. Moreover, he must often make operational decisions without waiting for complete information. Operational decisionmaking is inherently based on

taking *high but prudent risks*. The uncertainties regarding the enemy's intentions are much greater at the strategic and operational levels than at the tactical one.[40] The consequences of a failure at the operational level are much more severe than at the tactical level, and they cannot be overcome easily, if at all. At the same time, however, the potential gain is much greater at the operational and strategic levels of command than at the tactical level.

A willingness to take calculated risks has distinguished all the great leaders of the past. The attempt to fight a safe battle without taking risks has rarely been successful. The doctrine that leaves nothing to chance has not resulted in a decisive victory. For example, Admiral Horatio Nelson (1758–1805) was always taking great risks. Those who take big risks in war nearly always seem to have luck on their side.[41]

Willingness to take prudent risks means making operational decisions in varying degrees of uncertainty. Such decisions are critical for success, especially when one's forces are weaker than those of the enemy. They are not gambles, but carefully made calculated decisions. An operational commander often achieves success by taking reasonable risks. Clearly, there is never enough time or enough resources, and most choices involve some risks. There are no certainties in war.[42]

The operational commander should not arbitrarily decide what force size and mix should be employed to accomplish the assigned operational or strategic objective. In all circumstances he should use all the sources of military and nonmilitary power available or becoming available.[43] One is never too strong in a war if the aim is to achieve a quick and decisive victory.[44] There is simply no such a thing as being strong enough.[45] Hence, a decisive victory could come only by using one's *overwhelming strength*. The key prerequisite for success in combat is to be stronger than the enemy at the decisive point and to use speed, surprise, and deception. Admiral Nelson believed that only numbers could annihilate. Napoleon I remarked, "God is on the side of the big battalions." Neither Napoleon I nor Nelson thought in terms of strength superiority overall. What they aimed at was to employ their available forces so that they could fall in overwhelming force on a portion of the enemy and, having defeated it, do the same to some other part.[46] The commander who tries to be strong everywhere or who wastes his forces on secondary missions acts contrary to this basic rule.[47]

One of the key prerequisites for success in both operations short of war and high-intensity conventional war is quality and skills of commanders and rank and file. The higher the level of command, the more critical it is to have highly educated, trained, and skilled commanders and staffs. Among other things, an operational commander should have strong character, moral courage, boldness, creativity, and an uncanny ability to think operationally instead of tactically. Experience shows that there were only few leaders who had some inborn qualities to think broadly and far ahead into the future. For most successful commanders, operational thinking was acquired through consistent efforts in times of peace. Professional education, self-education in particular, and training are the principal means of obtaining operational thinking. The tenets of operational leadership should not be applied like a dogma but based on the mission and situation. Experience shows that overemphasis on technology at the expense of operational thinking cannot lead to success against a strong opponent. In a war between two strong opponents, victory will go to the side that thinks better and acts faster and with greater determination. **JFQ**

Notes

[1] Field Manual (FM) 22-103, *Leadership and Command at Senior Levels* (Washington, DC: Headquarters Department of the Army, June 21, 1987), 3.

[2] Cited in Brian Howieson and Howard Kahn, "Leadership, Management and Command: The Officer's Trinity," in *Airpower Leadership: Theory and Practice*, ed. Peter W. Gray and Sebastian Cox (London: The Stationery Office, 2002), 23.

[3] Richard A. Gabriel, *The Antagonists: A Comparative Combat Assessment of the Soviet and American Soldier* (Westport, CT: Greenwood Press, 1984), 83.

[4] Werner W. Banisch, "Leadership at the Operational Level," *Army* 8 (August 1987), 60.

[5] David Jablonsky, "Strategy and the Operational Level of War: Part I," *Parameters* (Spring 1987), 71.

[6] This term has many meanings and is extensively used in both military and civilian world. In one military definition, *situational awareness* pertains to "a pilot's (or aircrew's) continuous perception of self and aircraft in relation to the dynamic environment of flight, threats, and mission, and the ability to forecast, then execute tasks based on that perception." See Aaron W. Schopper, "Measuring situational awareness of AWACS weapons directors," *Situational Awareness in the Tactical Air Environment: Augmented Proceedings of the Naval Air Warfare Center's First Annual Symposium, CSERIAC SOAR Report# 97-01*, Wright-Patterson Air Force Base, OH, July 1997.

[7] General Johann von Kielmansegg, cited in Norbert Hanisch, *Untersuchen Sie die operativen Ideen Manstein hinsdichtlich Schwerpunkt-bildung, Ueberraschung, Initiative und Handlungsfreiheit an den Beispielen Westfeldzug 1940 (Sichelschnitt-Plan) und Operation Zitadelle* (Hamburg: Fuehrungsakademie der Bundewehr (FüAkBw), January 15, 1988), 4.

[8] Ibid., "Motto."

[9] Daniel J. Hughes, ed., *Moltke on the Art of War: Selected Writings* (Novato, CA: Presidio, 1993), 184.

[10] Gérard Chaliand, *The Art of War in World History: From Antiquity to the Nuclear Age* (Berkeley: University of California Press, 1994), 768.

[11] Robert W. RisCassi, "Doctrine for Joint Operations in a Combined Environment: A Necessity," *Military Review* 77, no. 1 (January–February 1997).

[12] Thomas E. Ricks, *The Generals: American Military Command from World War II to Today* (New York: Penguin, 2012), 177.

[13] Edward N. Luttwak, "The Operational Level of War," *International Security* 5, no. 3 (Winter 1980–1981), 62.

[14] Heinrich Merkens, *Ausgewaehlte Kriegswissenschaftliche Schriften Friedrichs des Grossen* (Jena: Hermann Costenoble, 1876), 7.

[15] "The Instruction of Frederick the Great for His Generals 1747," trans. Raphael T. Phillips, in *Roots of Strategy: A Collection of Military Classics* (Harrisburg, PA: Military Service Publishing, 1940), 314.

[16] Ludwig Freiherr Ruedt von Collenberg, *Die Geschichte des Preussisch–Deutschen Generalstabes von seinene Anfaengen bis zum Ende des ersten Weltkrieges-Beilagen*, 2nd part, P-135, ZA/1 2106, Studien der Historical Division Headquarters, United States Army Europe, Foreign Military Studies Branch, BA-MA, 155–156.

[17] William Slim, "Higher Command in War," *Royal Air Force Quarterly* 2 (April 1953), 149.

[18] *Generalfeldmarschall Graf von Moltke Ausgewaehlte Werke*, Vol I: *Feldherr und Kriegslehrmeister* (Berlin: Berlag von Reimar Hobbing, 1925), 55.

[19] Erich H. Koenen, *Die operativen Ideen Mansteins hinsichtlich Nuetzung des Raumes, Gewinnen der Initiative, Schaffen von Handlungsfreiheit und Wahl zwischen offensivem and defensivem Vorgehen. Eine Untersuchung anhand der Beispiele "Rochade" und Schlacht bei Kharkow des Winterfeldzuges 1942/43* (Hamburg: FüAkBw, November 1988), 2; FüAkBw, "Operative Leitlinie fuer die Fuehrung von Landstreitkraeften" (October 1993), Arbeitspapier, *Operative Fuehrung* (Hamburg: FüAkBw, August 1992), 19; Eike Middeldorf, *Fuehrung und Gefecht: Grundriss der Taktik* (Frankfurt, a.M: Bernard & Graefe, Verlag fuer Wehrwesen, 1968), 51.

[20] Alfred Gause, "Command Techniques Employed by Field Marshal Rommel in Africa," *Armor* 4 (July–August 1958), 23.

[21] Lothar Rendulic, *Grundlagen militaerischer Fuehrung* (Herford/Bonn: Maximilian Verlag, 1967), 51.

[22] Herbert Richmond, *National Policy and Naval Strength and Other Essays* (London: Longmans, Green, 1934), 285, 288–289.

[23] C.C. Carmine, "The Qualifications for Leadership," *Proceedings* 6 (June 1921), 858–859.

[24] Hughes, 1.

[25] B.H. Liddell Hart, *Strategy* (New York: Praeger, 1954), 348.

[26] Hanisch, 2.

[27] Arbeitspapier, *Operative Fuehrung* (Hamburg: FüAkBw, August 1992), 18.

[28] Christian Leggemann, *Die taktisch/operativen Ideen Mansteins hinsichtlich Schwerpunktbildung, Ueberraschung, Initiative und Handlungsfreiheit* (Hamburg: FüAkBw, January 4, 1989), 2.

[29] Arbeitspapier, 18.

[30] Eberhard Fuhr, *Die Handlungsfreiheit der militaerischen Fuehrung-Moeglichkeiten und Grenzen aufgrund des heutigen Kriegsbildes* (Hamburg: FüAkBw, February 16, 1968), 3.

[31] Paul K. Van Riper and F.G. Hoffman, "Pursuing Real Revolution in Military Affairs: Exploiting Knowledge-Based Warfare," *National Security Studies Quarterly* 4, no. 3 (Summer 1998), 11–12.

[32] Hughes, 132–133.

[33] "Auftragstaktik und Dienstaufsicht. Zwei Seiten derselben Medaille," *Truppendienst* 4 (July–August 1998), 310; Heinz Loquai, "Die Auftragstaktik als militaerische Fuehrungskonzeption," *Truppenpraxis* 6 (June 1980), 445.

[34] Van Riper and Hoffman, 11–12.

[35] Walter von Lossow, "Auftragstaktik am Beispiel der Operationsfuehrung einer Division des Heeres (Kurzfassung)," in Joachim Loeser, ed., "Moeglichkeiten und Grenzen der Auftragstaktik in unserer," *Rundschau* 5 (May 1976), 147.

[36] John F. Antal, "Forward Command: The Wehrmacht's Approach to Command and Control in World War II," *Armor* (November–December 1991), 28.

[37] John T. Nelsen II, "*Auftragstaktik*: A Case for Decentralized Battle," *Parameters* (September 1987), 25.

[38] Wolfgang Thomas, "Auftragstaktik. Voraussetzungen, Grenzen und Moeglichkeiten," *Wehrkunde* 11 (November 1968), 591.

[39] Werner Widder, "Auftragstaktik and Innere Fuehrung: Trademarks of German Leadership," *Military Review* 5 (September–October 2002), 5.

[40] Arbeitspapier, 18.

[41] Russell Grenfell, *The Art of the Admiral* (London: Faber and Faber, 1937), 134–135.

[42] FM 22-103, 33.

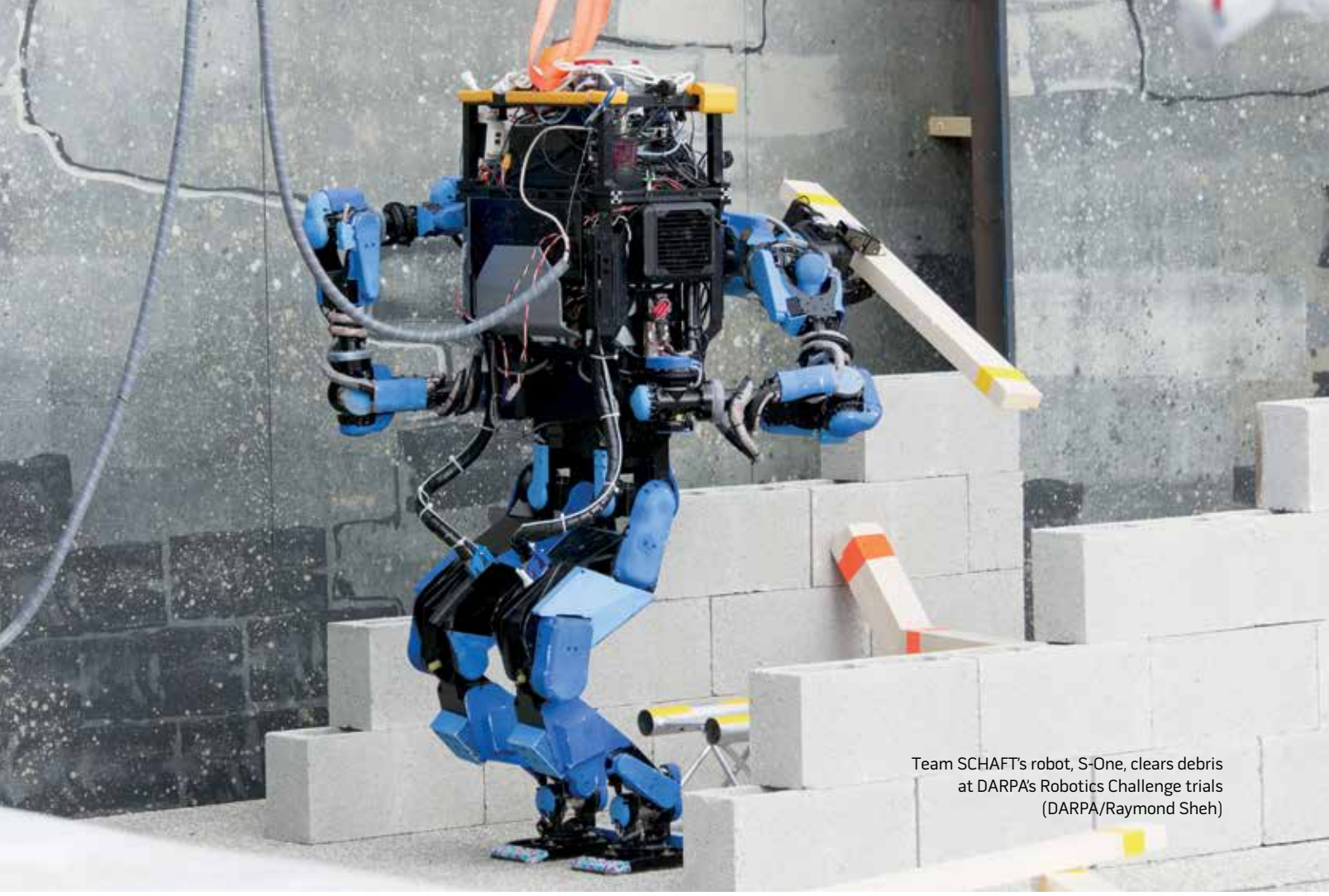
[43] Hughes, 219.

[44] Wilhelm Stanger, *Grundzuege der Lehre von der Strategie. Studienbehelf fuer die K.K. Kriegsschule*, Vol. 1: *Theorie mit Kuerzeren Bespielen* (Vienna: Verlag der K.K. Kriegschule, 1884), 15.

[45] Arbeitspapier, 17.

[46] Grenfell, 179.

[47] Bruce Condell and David T. Zabecki, eds., *On the German Art of War: Truppenfuehrung* (Boulder, CO: Lynne Rienner, 2001), 22.



Team SCHAFT's robot, S-One, clears debris at DARPA's Robotics Challenge trials (DARPA/Raymond Sheh)

Relying on the Kindness of Machines?

The Security Threat of Artificial Agents

By Randy Eshelman and Douglas Derrick

Modern technology is a daily part of our lives. It serves critical functions in defense, responding to natural disasters, and scientific research. Without technology, some of the most common human tasks would become laborious or, in many cases, impossible. Since we have become dependent on technology and its uses, and technology is becoming ever more capable, it is necessary that we consider the possibility of goal-driven, adaptive agents becoming an adversary instead of a tool.

We define *autonomous, adversarial-type technology* as existing or yet-to-be-developed software, hardware, or architectures that deploy or are deployed to work against human interests or adversely impact human use of technology without human control or intervention. Several well-known events over the last two decades that approach the concept

Randy Eshelman is Deputy of the International Affairs and Policy Branch at U.S. Strategic Command. Dr. Douglas Derrick is Assistant Professor of Information Technology Innovation at the University of Nebraska at Omaha.

Table. Adversarial Technology Examples

Adversarial Technology	Year	Financial Impact	Users Affected	Transmit Vector
"I Love You"	2000	$15 billion	500,000	Emailed itself to user contacts after opened
"Code Red"	2001	$2.6 billion	1 million	Scanned Internet for Microsoft computers—attacked 100 IP addresses at a time
"My Doom"	2004	$38 billion	2 million	Emailed itself to user contacts after opened
Stuxnet	2010	Unknown	Unclear	Attacked industrial control systems
"Heartbleed"	2014	Estimated tens of millions	Estimated at 2/3 of all Web servers	Open Secure Sockets Layer flaw exposes user data

Sources: "Top 5 Computer Viruses of All Time," UKNorton.com, available at < http://uk.norton.com/top-5-viruses/promo>; "Update 1—Researchers Say Stuxnet Was Deployed Against Iran in 2007," Reuters, February 26, 2013, available at <www.reuters.com/article/2013/02/26/cyberwar-stuxnet-idUSL1N0BQ5ZW20130226>; Jim Finkle, "Big Tech Companies Offer Millions after Heartbleed Crisis," Reuters, April 24, 2014, available at <www.reuters.com/article/2014/04/24/us-cybercrime-heartbleed-idUSBREA3N13E20140424>.

of adversarial technology are the "I Love You" worm in 2000, the "Code Red" worm in 2001, the "My Doom" worm in 2004, and most recently, the "Heartbleed" security bug discovered in early 2014. Similarly, the targeted effects of Stuxnet in 2010 could meet some of the requirements of dangerous autonomous pseudo-intelligence. As shown in the table, these technologies have serious consequences for a variety of users and interests.

While these and other intentional, human-instigated programming exploits caused a level of impact and reaction, the questions that this article addresses are these: What are the impacts if the adaption was more capable? What if the technologies were not only of limited use but were also actively competing with us in some way? What if these agents' levels of sophistication rapidly exceeded that of their developers and thus the rest of humanity?

Science fiction movies have depicted several artificial intelligence (AI) "end-of-the-world" type scenarios ranging from the misguided nuclear control system, "W.O.P.R.—War Operation Plan Response"—in the 1983 movie *War Games*, to the malicious Terminator robots controlled by Skynet in the series of similarly named movies. The latter depict what is widely characterized as the *technological singularity*, that is, when machine intelligence is significantly more advanced than that of human beings and is in direct competition with us.

The anthropomorphizing of these agents usually does make for box office success. But this is potentially hazardous from a policy perspective as noted in the table. Hostile intent, human emotion, and political agendas were not required by the adversarial technologies themselves in order to impact users. Simple goals, as assigned by humans, were sufficient to considerably influence economies and defense departments across the globe. Conversely, many nonfiction resources offer the alternative concept of a singularity—very advanced AI—benefiting humankind.[1] Human life extension, rapid acceleration of nanotechnology development, and even interstellar travel are often named as some of the projected positives of super intelligent AI.[2] However, other more wary sources do not paint such an optimistic outlook, at least not without significant controls emplaced.[3] As Vernor Vinge (credited with coining the term *technological singularity*) warned, "Any intelligent machine [referring to AI] . . . would not be humankind's 'tool' any more than humans are the tools of rabbits or robins or chimpanzees."[4]

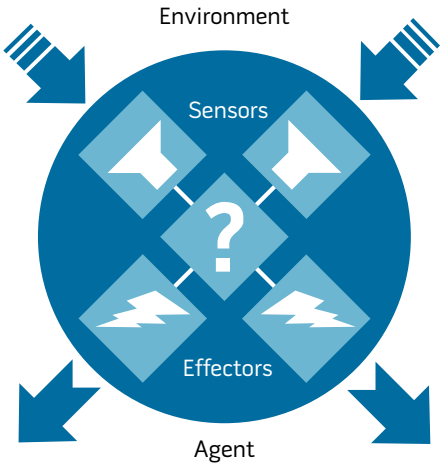
In this article, we offer a more pragmatic assessment. It provides common definitions related to AI and goal-driven agents. It then offers assumptions and provides an overview of what experts have published on the subject of AI. Finally, it summarizes examples of current efforts related to AI and concludes with a recommendation for engagement and possible actions for controls.

Definitions

Establishing definitions is basic to address risk appropriately. Below are generally accepted terms coupled with specific clarifications where appropriate.

- Artificial intelligence: The theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decisionmaking, and translation between languages.
- Artificial general intelligence (AGI)/human-level intelligence/strong AI: These terms are grouped for the purposes of this article to mean "intelligence equal to that of human beings"[5] and are referred to as AGI.
- Artificial super intelligence (ASI): "Intelligence greater than human level intelligence."[6]
- Autonomous agent: "Autonomy generally means that an agent operates without direct human (or other) intervention or guidance."[7]
- Autonomous system: "Systems in which the designer has not predetermined the responses to every condition."[8]
- Goal-driven agents: An autonomous agent and/or autonomous system with a goal or goals possessing applicable sensors and effectors (see figure).
- Sensors: A variety of software or hardware receivers in which a machine or program receives input from its environment.

Figure. Goal-Driven Agent Example Assumptions



- Effectors: A variety of software or hardware outlets that a machine or program uses to impact its environment.

Currently, it is generally accepted that ASI, AGI, or even AI do not exist in any measurable way. In practice, however, there is no mechanism for knowing of the existence of such an entity until it is made known by the agent itself or by its "creator." To argue the general thesis of potentially harmful, goal-driven technologies, we need to make the following assumptions concerning past technological developments, the current state of advances, and future plausible progress:

- Moore's Law,[9] which correctly predicted exponential growth of integrated circuits, will remain valid in the near term.
- Advances in quantum computing, which may dramatically increase the speed at which computers operate, will continue.[10]
- Economic, military, and convenience incentives to improve technologies and their uses will continue, especially in the cyberspace and AI fields.
- A global state of technological interconnectedness, in which all manners of systems, devices, and architectures are linked, will continue to mature and become more robust and nearly ubiquitous.

Defense and the Leading Edge of Technology

From the earliest days of warfare, those armies with the most revolutionary or advanced technology usually were the victors (barring leadership blunder or extraordinary motivations or conditions[11]). Critical to tribal, regional, national, or imperial survival, the pursuit of the newest advantage has driven technological invention. Over the millennia, this "wooden club-to-cyberspace operations" evolution has proved lethal for both combatants and noncombatants.

Gunpowder, for example, was not only an accidental invention but also illustrates an unsuccessful attempt to control technology once loosed. Chinese alchemists, searching for the secrets of eternal life—not an entirely dissimilar goal of some proponents of ASI research[12]—discovered the mixture of saltpeter, carbon, and sulfur in the 9th century. The Chinese tried, but failed, to keep gunpowder's secrets for themselves. The propagation of gunpowder and its combat effectiveness spread across Asia, Europe, and the rest of the world. The Byzantine Empire and its capital city of Constantinople, previously impervious to siege, fell victim to being on the wrong side of technology when the Ottoman Turks blew through the walled city with cannon in the 15th century.[13]

Information technology (IT)—from the telegraph, to satellite systems, to globally connected smart devices—has fundamentally altered the landscape of military and civil operations, much like gunpowder did in its day. Furthermore, IT allows the management of military resources and financial systems worldwide. From a defense perspective, it has become difficult to find a single function, application, plan, or asset not enabled or impacted by the use of IT. Information technology has become so paramount that the President has made the operation and defense of the U.S. military's portion of IT infrastructure a mission for military leadership at the highest levels.

U.S. Strategic Command's subordinate or subunified command, U.S. Cyber Command (USCYBERCOM), is the evolutionary result of IT advancement, dependence, and protection. The USCYBERCOM mission statement, in part, directs the command to "plan, coordinate, synchronize and conduct activities to operate and defend DoD information networks and conduct full spectrum military cyberspace operations."[14] This is a daunting task given the reliance on systems and systems of systems and the efforts to exploit these systems by adversaries. This mission statement does imply a defense of networks and architectures, regardless of specific hostile agents. However, the current focus seems to have an anti-hacker (that is, human, nation-state, terror group) fixation. It does not, from a practical perspective, focus on artificial agent activities explicitly.

IT has allowed us to become more intelligent. At a minimum, it has enabled the diffusion of knowledge at paces never imagined. However, IT has also exposed us to real dangers such as personal financial or identity ruin or cyberspace attacks on our industrial control systems. It is plausible that a sufficiently resourced, goal-driven agent would leverage this technology to achieve its goal(s)—regardless of humankind's inevitable dissent.

Review of the Literature

Stephen Omohundro, Ph.D. in physics and mathematics and founder of Self-Aware Systems, a think tank for analyzing intelligent systems, has written extensively on the dangers inherent in any autonomous system. He states, "Autonomous systems have the potential to create tremendous benefits for humanity . . . but they may also cause harm by acting in ways not anticipated by their designers. Such systems are capable of surprising their designers and behaving in unexpected ways."[15] Omohundro outlines basic AI drives inherent in a goal-driven agent: "Without special precautions, it will resist being turned off, will try to break into other machines and make copies of itself, and will try to acquire resources without regard for anyone else's safety . . . not because they were programmed in at the start, but because of the intrinsic nature of goal driven systems."[16] Omohundro's four basic AI drives are:

- Efficiency: This drive will lead to improved procedures for computational and physical tasks.
- Resource loss avoidance: This drive will prevent passive losses and prevent outside agents from taking resources.
- Resource acquisition: This drive may involve exploration, trading, or stealing.
- Increasing utility: This drive would be to search for new behaviors to meet desired goals.

Other examples of the basic drives would be:

- Efficiency: the shutting down of systems not currently necessary for goal achievement (for example, a tertiary power grid—from the AI's perspective—but a primary source for humans)
- Resource loss avoidance: a protection of assets currently needed or determined to be required in the future (for example, active protection of servers by automated locking and monitoring of physical barriers)
- Resource acquisition: financial market manipulation to gain fungible assets for later satellite access (for example, leasing of bandwidth for more efficient communications through extant online tools)
- Increasing utility: game-playing, modeling, and simulation-running to determine best approaches to achieving goal(s).

Nick Bostrom, Ph.D. in economics and director of the Oxford Martin Programme on the Impacts of Future Technology with Oxford University, states, "Since the superintelligence may become unstoppably powerful because of its intellectual superiority and the technologies it could develop, it is crucial that it be provided with human-friendly motivations."[17] Bostrom also discusses a potential for accelerating or retarding AI, AGI, and ASI development from a policy perspective. However, given the motivators already discussed in this article, an impeding of AI research and development would be problematic for a nation to undertake unilaterally and would almost certainly require more than policy statements.

CHIMP, from Tartan Rescue Team, placed third in the DARPA Robotics Challenge Trials 2013 (DARPA)

Eliezer Yudkowsky, co-founder of the Machine Intelligence Research Institute, states in a chapter of *Global Catastrophic Risks*, "It is far more difficult to write about global risks of Artificial Intelligence than about cognitive biases. Cognitive biases are settled science; one need simply quote the literature. Artificial Intelligence is not settled science; it belongs to the frontier, not to the textbook."[18] This exemplifies the revolutionary leaps that seem possible considering the rate of technological advances (Moore's Law) and the motivations of a potentially unknowable number of developers. Yudkowsky goes on to emphasize the dangers of anthropomorphic bias concerning potential risks associated with AI:

Humans evolved to model other humans—to compete against and cooperate with our own conspecifics. It was a reliable property of the ancestral environment. . . . We evolved to understand our fellow humans empathically, by placing ourselves in their shoes. . . . If you deal with any other kind of optimization process . . . then anthropomorphism is flypaper for unwary scientists.[19]

James Barrat, an author and documentarian with National Geographic, Discovery, and PBS, states, "Intelligence, not charm or beauty, is the special power that enables humans to dominate Earth. Now, propelled by a powerful economic wind, scientists are developing intelligent machines. We must develop a science for understanding and coexisting with smart, even superintelligent machines. If we fail . . . we'll have to rely on the kindness of machines to survive."[20] Barrat's "busy child" analogy depicts a developed AI system that rapidly consumes information and surpasses human-level intelligence to become an ASI. Its human overseers correctly disconnect the busy child from the Internet and networks because:

Legged Squad Support System (LS3) robots will go through same terrain as human squad without hindering mission (DARPA)

once it is self-aware, it will go to great lengths to fulfill whatever goals it's programmed to fulfill, and to avoid failure. [It] *will want access to energy in whatever form is most useful to it, whether actual kilowatts of energy or cash or something else it can exchange for resources. It will want to improve itself because that will increase the likelihood that it will fulfill its goals. Most of all, it will not want to be turned off or destroyed, which would make goal fulfillment impossible. Therefore, AI theorists anticipate our ASI will seek to expand out of the secure facility that contains it to have greater access to resources with which to protect and improve itself.*[21]

Current Efforts in AI and Autonomous Agents

The Defense Advanced Research Projects Agency (DARPA), established to "prevent strategic surprise from negatively impacting U.S. national security and create strategic surprise for U.S. adversaries by maintaining the technological superiority of the U.S. military,"[22] is the preeminent technological anticipator and solicitor with a defense focus. DARPA has incentivized such things as automated ground vehicle technology, robotics maturation, and cyber self-defense through a competition format, with prizes awarded in the millions of dollars. For example, the 2004 Grand Challenge offered a $1 million prize to the team whose automated, unmanned vehicle was able to traverse a difficult 142-mile desert trek in a specified amount of time. Although no team completed the course (and no prize money was awarded) in the 2004 event, the 2005 Grand Challenge saw a team from Stanford University not only claim the $2 million prize,[23] but also defeat the course in just 6 hours.

In March 2014, DARPA solicited entrants for its inaugural Cyber Grand Challenge to "enable DARPA to test and evaluate fully automated systems that perform software security reasoning and analysis."[24]

DARPA's Robotics Challenge (DRC) aims for contestant robots to demonstrate, in part, "Partial autonomy in task-level decision-making based on operator commands and sensor inputs."[25] The competition drew numerous contestants, both DARPA-funded and self-funded, with nine DARPA-funded candidates and two self-funded candidates still remaining in the competition as of May 2014. Interestingly, the highest scoring team from DARPA's December 2013 DRC trials, Team SCHAFT, has been acquired by Google, Inc., and has elected to self-fund.[26]

Much less information is available about private company endeavors into AI, automated agents, automated systems, or AGI/ASI. Google, however, should be considered a leader in at least the pursuit of the highest technologies. With its recent purchase of robotics companies such as Boston Dynamics[27]

and Team SCHAFT, its Google Glasses, the driverless car, and AI company DeepMind, Google's direction seems to point toward an AI or AI-like capability. An additional note and perhaps key indication of Google's AI focus was the hiring of Ray Kurzweil, noted futurist, AI authority, and author of *The Singularity Is Near: When Humans Transcend Biology*.

Douglas Derrick has conducted live autonomous agent tests using his Special Purpose, Embodied, Conversational Intelligence with Environmental Sensors (SPECIES) agent. His agent-based system builds on existing communications models and theories and interacts directly with humans to achieve the goal of essentially discerning human deceit. Dr. Derrick writes of the "natural progression of human interactions with machines,"[28] where systems (machines) are being developed or will be developed that may assess human states, to include whether or not the human is being truthful. Derrick's prototype SPECIES agent was built to interview potential international border crossers as they passed through security lines. His team conducted a field study using his SPECIES agent with U.S. Customs and the Federal Bureau of Investigation, where the SPECIES agent was to "evaluate physiological and behavioral deviations from group and individual baselines in order to discriminate between truthful and deceitful communication."[29] Derrick's work demonstrated, to some degree, a goal-driven agent's ability not only to interact with humans, but also to engage in a level of persuasiveness while interacting with humans.

Conclusion and Recommendation

This article is not intended to be alarmist. On the contrary, it should serve as an initial call for engagement and collaboration. AI, AGI, ASI or the technological singularity may never come to fruition. Perhaps machines will plateau at or near where we are currently positioned in terms of nonhuman intelligence. Or perhaps a friendly version of AI will be developed and "decide" serving humankind obliges its own self-interests. Either of these possibilities is within the realm of reason. Yet considering the incentives and the demonstrated advances in a relatively short period of time, a more pragmatic view would suggest an approach more akin to cautious optimism. Once the possibility of goal-driven agents is considered, it does become easier to envision impacts being realized at some level.

This article recommends that the Department of Defense establish a working group concentrating on defense and industry engagement pertaining to goal-driven agents and artificial intelligence. This working group should have a basic charter to research current U.S. and partner efforts in AI and provide formal feedback to defense officials and policymakers. Similarly, there must be a call for research into codifying ethics and moral behavior into machine logic. The philosophical considerations that help define human morality must be able to be codified and expressed to nonhuman intelligences. Research should be conducted to temper goal-driven, autonomous agents with ethics. Basic research must be undertaken into what this codification and expression could be. JFQ

Notes

[1] Peter H. Diamandis and Steven Kotler, *Abundance: The Future Is Better Than You Think* (New York: Free Press, 2012).

[2] Ray Kurzweil, *The Singularity Is Near: When Humans Transcend Biology* (New York: Penguin, 2005).

[3] James Barrat, *Our Final Invention: Artificial Intelligence and the End of the Human Era* (New York: Macmillan, 2013).

[4] Vernor Vinge, "The Coming Technological Singularity: How to Survive in the Post-Human Era," 1993, available at <www-rohan.sdsu.edu/faculty/vinge/misc/singularity.html>.

[5] Barrat.

[6] Ibid.

[7] Michael Wooldridge and Nicholas R. Jennings, "Agent Theories, Architectures, and Languages: A Survey," in *ECAI-94 Proceedings of the Workshop on Agent Theories, Architectures, and Languages on Intelligent Agents* (New York: Springer-Verlag, 1995), 1–39.

[8] Stephen Omohundro, "Autonomous Technology and the Greater Human Good," *Journal of Experimental and Theoretical Artificial Intelligence* 26, no. 3 (2014), 303–315.

[9] David R.S. Cumming, Stephen B. Furber, and Douglas J. Paul, "Beyond Moore's Law," *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 372 (2012), available at <www.ncbi.nlm.nih.gov/pmc/articles/PMC3928907/>.

[10] Jeremy Hsu, "Quantum Bit Stored for Record 39 Minutes at Room Temperature," *Institute of Electrical and Electronics Engineers Spectrum*, November 15, 2013, available at <http://spectrum.ieee.org/tech-talk/computing/hardware/quantum-bit-stored-for-record-39-minutes-at-room-temperature>.

[11] Saul David, *Military Blunders* (London: Constable & Robinson, 2014).

[12] Kurzweil.

[13] Jonathan Harris, *A Chronology of the Byzantine Empire*, ed. Timothy Venning (New York: Palgrave Macmillan, 2006).

[14] United States Strategic Command, "U.S. Cyber Command," available at <www.stratcom.mil/factsheets/2/Cyber_Command/>.

[15] Omohundro, "Autonomous Technology."

[16] Stephen M. Omohundro, "The Basic AI Drives," *Frontiers in Artificial Intelligence and Applications* 171 (2008), 483.

[17] Nick Bostrom, "Ethical Issues in Advanced Artificial Intelligence," *Science Fiction and Philosophy: From Time Travel to Superintelligence*, ed. Susan Schneider (Malden, MA: Blackwell Publishing, 2009), 277–284.

[18] Eliezer Yudkowsky, "Artificial Intelligence as a Positive and Negative Factor in Global Risk," in *Global Catastrophic Risks*, ed. Nick Bostrom and Milan Cirkovic (Oxford: Oxford University Press, 2008).

[19] Ibid.

[20] James Barrat, "About the Author," available at <www.jamesbarrat.com/author/>.

[21] Barrat, *Our Final Invention*.

[22] Defense Advanced Research Projects Agency (DARPA), "Our Work," available at <www.darpa.mil/our_work/>.

[23] DARPA, "Robotics Challenge," available at <www.theroboticschallenge.org/about>.

[24] DARPA, "Solicitation," available at <www.fbo.gov/index?s=opportunity&mode=form&id=328908705d152877b2022b72735c266f&tab=core&_cview=0>.

[25] DARPA, "Robotics Challenge."

[26] Ibid.

[27] Jonathan Berr, "Google Buys 8 Robotics Companies in 6 Months: Why?" CBS News, December 16, 2013, available at <www.cbsnews.com/news/google-buys-8-robotics-companies-in-6-months-why/>.

[28] Douglas C. Derrick, Jeffrey L. Jenkins, and Jay F. Nunamaker, Jr., "Design Principles for Special Purpose, Embodied, Conversational Intelligence with Environmental Sensors (SPECIES) Agents," *AIS Transactions on Human-Computer Interaction* 3, no. 2 (2011), 62–81.

[29] Ibid.

Robotic exoskeletons for warfighters help reduce injuries and fatigue and improve Soldiers' abilities to perform missions efficiently (DARPA/Boston Dynamics)

Will Humans Matter in the Wars of 2030?

By Andrew Herr

Much of the future-looking discussion in national security circles today focuses on autonomous systems and cyber weapons. Largely missing from this discussion is a place for humans on the battlefield. Do today's emerging and potentially disruptive technologies mean that humans will no longer be important in future warfare? A look at historical military operations and current technologies suggests the proper response is that, to paraphrase Mark Twain, reports of man's obsolescence have been exaggerated.

Back to the Future?

This is not the first time analysts have argued that human performance would be significantly less important in future combat. Stepping back to the 1960s, Navy and Air Force planners saw the radar and air-to-air missile age as forcing humans to take a backseat to technology. Missiles were the unmanned aerial vehicles (UAVs) of their day—unmanned, high-tech systems to match the speed and technology of advanced warfare. In their proponents' vision, fighters would not get close enough to each other for dogfighting skills to matter, so the U.S. military largely discontinued specialized air-combat tactics

Andrew Herr is the CEO of Mind Plus Matter, a human performance consulting firm, and Helicase, a technology consulting firm. He works with a range of commercial and government clients to enhance mental and physical performance and to develop research and development strategies.

training and even purchased the F-4 fighter without an internal gun.

The Vietnam War proved to be a rude awakening for the aviation community. The Navy and Air Force expected to have a major advantage over the North Vietnamese air force, but both Services were losing one plane for every two they destroyed in the first half of the air war. By 1969, both had serious initiatives to improve their performance. The Air Force diagnosed a failure of technology, and it spent its resources on improving missile and aircraft performance. In contrast, the Navy identified a failure in training. This led the Navy to establish the Navy Fighter Weapons School (better known as TOPGUN), which gave pilots realistic air combat training. The results speak for themselves. From 1970 to 1973, the Navy was killing more than 12 North Vietnamese planes for every loss, while the Air Force had not improved at all.[1]

While this demonstrates the importance of humans in the context of 1970s technology, will 2030s technologies change this calculus?

Insights from Future-Looking Wargames

Some potential answers to this question flow from a series of recent wargames sponsored by the Department of Defense (DOD) Rapid Reaction Technology Office. To identify what DOD should watch closely, the NeXTech wargames focused on technology trends by examining how the United States and competitors might use them (and might use them differently), their potential impact, and the legal, ethical, and policy issues these technologies could generate.

First and foremost, the structure of the wargames shows some areas where we rely on humans and are likely to continue doing so. While focused on future technologies, the wargames did not look anything like the futuristic military environment. Participants gathered in conference rooms to discuss scenarios outlined on paper. Although some wargames use computer simulations and sophisticated data presentation, the NeXTech environment is representative of the majority of wargames conducted for DOD. This is not intended to be a criticism; the structure made sense because the focus was on extracting ideas and judgments *from people*, not computer simulations. We still rely on human expertise because computers simply cannot match it.

The same is true of intelligence analysis. While analysts use software and other tools to aid their work, the final judgment lies in the hands of people. The story of Palantir Technologies, a high-flying provider of software to the U.S. national security community, highlights this. The story begins in the early days of PayPal. The Russian mafia and other criminal organizations were stealing so much money through fraudulent transactions that PayPal was in danger of failing. As a Silicon Valley–based company, PayPal's management hired top computer scientists coming out of Stanford to design an automated system to catch fraudulent transactions, but initial attempts failed. PayPal succeeded only when the programmers changed course and designed a system whose purpose was not to *solve* the problem, but to help humans sort through large amounts of data to identify fraud. This software and the approach behind it gave birth to Palantir. If the growth of Palantir Technologies within the national security and commercial space is any measure, myriad organizations agree.

Google's autonomous cars also demonstrate the value of human input to computers. Image recognition systems cannot effectively pick out a stoplight while driving down a street, but once programmers give the location of street lights to a computer, it is a trivial job to identify whether it is red, yellow, or green.[2] Thus, today, humans are instrumental, and a broader lesson appears: there are tasks where humans excel and those where computers exceed human capabilities, and computers appear unlikely to close many of these gaps by 2030, even with research on cognitive computing and the structure of the brain progressing.

In a 2012 paper, even a group of leading scientists in neuroscience and biology argued that we are still in the early days of this work. Researchers still principally focus on single neurotransmitters (which act to carry certain messages in the brain) and a few neurons at a time, while there are approximately 100 neurotransmitters and 100 billion neurons that interact in ways that create emergent properties. Multiple highly funded research projects are starting or have recently started to develop a more holistic understanding of the brain. These will advance the field, but as Santiago Ramon y Cajal, one of the fathers of neuroscience, described, the neurons and the synapses can be like "impenetrable jungles where many investigators have lost themselves."[3]

This is not to say that we should not be vigilant for unanticipated, nonlinear advances in science and technology, but today's scientific and technological landscape suggests that the human brain will still substantially outperform computers in the highest level cognitive tasks in 2030. Furthermore, the competition is not simply between the brain and computers, but rather between computers and humans *augmented by* computers.

Humans or Computers? Both.

Gary Kasparov and the world of chess provide a valuable insight into the human-computer relationship. After decades of humans easily beating computers, Kasparov barely beat IBM's Deep Blue machine in 1996, and a year later, the IBM computer won. The enormous computational power of computers could outmatch the best humans. This is not, however, the end of the story. Fascinated by the power of computers, but still recognizing the strengths of the human brain, Kasparov began to organize what he called Advanced Chess, games where human-computer teams competed against one another. Even as chess computers advanced, humans with relatively simple chess programs dominated chess-specific supercomputers. Perhaps even more interestingly, the winners are not necessarily grandmasters with high-end computers. In early tournaments, the organizers were surprised to find that chess novices who were expert at manipulating the computers beat the

grandmasters with their computers.[4] Thus, while the type of skills required changed, the human brain still gave a major advantage.

New approaches to computer algorithms and interface design will continue to enhance the joint performance of humans and computers, so for autonomous computers to reach primacy, their development will have to outpace not only humans, but also the advancing performance of human-computer teams. Taken together, these examples strongly suggest that areas such as operational planning, intelligence analysis, and command will almost certainly stay within the human realm.

Stuck at the Back Making Decisions?

While planning, command, and intelligence analysis are all crucial aspects of war, they only represent a fraction of the roles military personnel fill today, and they might be pushed to the rear *if* autonomous systems controlled the battlefield. However, as long as humans have an advantage in the areas of creativity and judgment, we will have a major role at the frontlines. Today's special operations missions are one example: when missions have a significant degree of uncertainty, require the ability to adapt on the fly, and have the chance for major reversals, the adaptability of humans is invaluable.

Consider the complexity of the Osama bin Laden raid. Almost immediately upon arrival, one of the helicopters crashed. Once the special operators entered the compound, they needed to protect themselves (just as machines would need to), but they did not want to kill unarmed women and children, so they had to operate based on a combination of tactical and ethical inputs. Then people from the neighborhood started to approach the compound, and the team needed to handle an additional potential threat. Meanwhile, the mission not only required the identification and killing or capturing of bin Laden, but it also proceeded to an intelligence collection mission, collecting computers and files.

While it is possible to program some of these activities and contingencies into autonomous systems, this is no simple task, and we are still far from a world where autonomous systems can face the essentially unlimited complexity of the modern battlefield with the skill of humans. It appears that, for some time into the future, humans will continue to excel in diverse missions such as this one. Certainly, the bin Laden raid was special in terms of importance and sensitivity, but all military missions require multiple judgment calls and adaptations throughout their length, whether or not they are undertaken by special operators. To some extent, commanders could direct systems remotely, but the human brain is tailored to operate in conjunction with our senses, so not being present may rob humans—and thus, our human-computer teams—of part of our effectiveness. Being on the battlefield also enables human-human interaction, which is important for interaction with local populaces and, to some extent, with enemy forces, such as captured soldiers.

Furthermore, remote control requires connectivity, and this is not guaranteed on the battlefield of today or tomorrow. The issue of connectivity and the value of having military personnel in the midst of operations are highlighted by some of the very same technology trends that commentators suggest have the potential to replace traditional human roles. The simultaneous belief in the future effectiveness of autonomous systems *and* effective cyber tools is striking.

During one scenario played out in the NeXTech wargames, a fictional naval force sailed toward an island chain that the wargamers were assigned to defend. To do so, they chose to deploy cyber tools against the ships' command and control systems to wreak havoc with their defensive systems and disable their engines in a sort of "on demand" Stuxnet attack. If the United States—or potential adversaries—is able to achieve this level of effectiveness with cyber tools, autonomous systems may be especially vulnerable because of the lack of humans in the loop who might be able to override certain commands or at least recognize that something is amiss. This creates a cyber-autonomy paradox: powerful cyber tools can turn autonomous systems, usually an asset, into a liability.

Humans are in no way perfect, of course, but our ability to identify patterns and integrate information holistically is superior to computers in many situations and is a tool that can help maintain situational awareness. Furthermore, without humans in the loop, it may be difficult for commanders to know when systems have been compromised, as feedback from a compromised system may not accurately represent its status, location, or activities. Humans will not be able to intervene against all types of attacks—shutting down an engine on an aircraft would still be catastrophic—but we may be able to intervene against misleading signals from sensors and other challenges.

The value of this is highlighted by a number of stories from the past few years that demonstrate that not all aspects of military systems are protected. In 2009, the media reported that Iraqi insurgents were viewing the video recorded by Predator UAVs in Iraq using $26 software because the signals transmitting the video to personnel on the ground were not encrypted.[5] This particular weakness might not make the systems vulnerable, but it shows the difficulty of mitigating all potential weaknesses. Furthermore, it is worth remembering Joy's Law (named after the founder of Sun Microsystems, Bill Joy), which states that in all cases, the majority of the best people work for someone else. No matter how good our systems are, the majority of the best cyber operators and hackers will always be outside DOD.

Thus, while humans are hardly a cure-all for cyber attacks—we often enable the attacks by clicking on the wrong link or using flash drives—people may be able to mitigate the impact of certain types of attacks, such as inaccurate location information being fed into systems. We may also be able to communicate the problem so that commanders can engage defensive teams and systems to mitigate the effects of attacks. This does not mean that humans need to be on every platform, but it does suggest that it will be important to have humans near the frontlines.

The value of keeping humans in the loop to respond to erroneous data is perhaps best illustrated by the story of Stanislav Petrov. Then a lieutenant colonel in the Soviet Air Defense Forces, he was the duty officer overseeing the Soviet early warning satellite system in September 1983 when he was alerted that the United States had launched a handful of intercontinental ballistic missiles. Tensions were high at the moment; the Soviet Union had shot down a South Korean airliner only weeks before, and the United States was about to begin major military exercises, which included nuclear weapons. However, Petrov did not believe the system. He figured that the United States would not launch a small number of missiles in a first strike. Ground radars did not corroborate the report, and he recognized the potential for the new satellite sensors and computer system to make a mistake. He declared it a false alarm, and in doing so, he prevented the alarm from potentially leading Soviet leaders to order nuclear retaliation. The cause of the false alarm was sunlight reflecting off high-altitude clouds.[6]

The Value(s) Proposition

Finally, cost, cost effectiveness, and bureaucracy will influence human roles. Humans are expensive because of the cost to train, house, feed, clothe, pay, treat, and insure military personnel, but machines cost money, too. For states or organizations without substantial resources, using humans is practical because it does not require the often very large, upfront, fixed cost of additional hardware. Furthermore, like humans, machines have ongoing costs for development, testing, upgrades, fuel, and maintenance. This means that humans are often more cost effective, even for well-funded military organizations, in positions where the technological solution is expensive or not yet mature. Looking at today's technology, this still covers the *vast majority* of positions humans fill, and this appears likely to continue to 2030. Even if there is no longer a pilot in the cockpit of many drones, there are still hundreds of humans supporting each mission, from analysis to maintenance.

First Air Force pilot qualified to fly F-35 secures helmet prior to stepping to F-35A Lightning II joint strike fighter at Eglin Air Force Base (U.S. Air Force/Samuel King)

The issue of cost effectiveness is also influenced by bureaucratic tendencies. When looking at DOD, it is clear that there is a preference for more capable, more expensive technological systems. A graph often circulated in defense circles—Norman Augustine's Law #16—shows that each successive aircraft DOD purchases is more expensive than the last and that we buy fewer units. A trend line on the graph points to a future where we will procure one aircraft, which will consume the entire defense budget. This tendency will push the United States away from cheaper disposable systems, which will likely further delay the day in which robots are more cost effective than humans in a range of roles.

The role of humans is also influenced by cultural factors within military organizations. The ethos of the warfighter is central to the culture of the military Services. While there are variations to each—pilots, submariners, Marines, and

LGM-118A Peacekeeper missile system tested at Kwajalein Atoll in Marshall Islands shows paths of multiple re-entry vehicles deployed by missile (U.S. Army/David James Paquin)

myriad others have their own mythologies—human traits such as bravery, skill, and honor are integral to their culture. So even as technology changes, cultures, which tend to change slowly without severe outside shocks, would have to change as well to significantly dislodge humans from the conduct of warfare.

Beyond Effectiveness: Social and Ethical Issues

A unique aspect of the NeXTech wargame series was the composition of the participants and the focus of one of the events on the ethical, legal, and policy implications of emerging technology. Almost all DOD wargames include military personnel and technical experts, but the NeXTech series also included journalists, lawyers, philosophers, and ethicists. As some of these participants have written about in other fora, autonomous technologies challenge our legal and ethical requirements to protect noncombatants and act discriminately.

In a scenario where a North Atlantic Treaty Organization–like force had to liberate a city from a conventional opposing force, participants debated how to approach the use of autonomous systems when targets were in close proximity to civilians. One participant asked, "If an autonomous system [accidentally] kills a civilian, is the commander responsible? The company that built the system? The individual who wrote the software code?" DOD has acknowledged this challenge at the highest levels, and it released special policy guidance on the development of lethal autonomous systems in a memorandum from the Deputy Secretary of Defense in November 2012.[7]

This is not to say that humans are free of mistakes but rather that we have accepted ethical, legal, and policy constructs to handle human error. This suggests that, even with the option to employ hypothetical highly effective military systems, we expect to continue to rely on humans in situations characterized by uncertainty for sociocultural reasons in addition to operational reasons. Looking to 2030, it seems unlikely that we will successfully be able to design, build, and trust autonomous systems with ethics *and* strategy hardcoded into them across the wide range of missions necessary to largely replace humans. Science fiction provides a number of insights into the challenges to doing so effectively.

But How Will We Keep Up?

While humans are likely to play a crucial role in the military operations of 2030, technologies will change the types of performance militaries require, and they may also change humans. To better handle the amount of data that sensors and systems provide about the battlefield, we will develop software and hardware systems to improve commanders' and operators' situational awareness—an example of human-plus-computer teams described above. For example, the F-35 pilot interface does not primarily rely on a heads-up display. Rather, the information display is built into the helmet so that wherever the pilot physically looks the system provides information. Even looking down provides a view of the ground from cameras with information overlaid on the visual, such as waypoints and enemy and friendly systems. While rife with problems throughout its development, by integrating multiple data feeds into the visual picture, the final version will hopefully enable the pilot to make better tactical decisions.

As is clear from the TOPGUN and Advanced Chess examples, training individuals to use technology will play a key role in enhancing effectiveness. As such, it will be important for militaries to invest in new simulation and training techniques, as well as to measure the effectiveness of these approaches. Measuring learning is only one aspect—measuring the *effect* of that learning is harder and almost certainly more important. At present, this is an area of weakness for the U.S. military, as performance is only rarely assessed in the context of how inputs such as training influence it, especially in realistic operational scenarios. While appropriate training can better enable military personnel to use technology, it will also be important to equip military personnel with the skills necessary to operate in the absence of certain systems—in line with the earlier discussion about the cyber-autonomy paradox. The need for navigation, air-traffic control, and myriad other areas in which military forces currently rely on technological systems will not cease due to digital disruption. Rather, operating in a technology-denied environment may be the critical skillset in future wars between sides that both possess high-end capabilities.

While these systems are likely to help, the amount of information, even if provided through well-designed systems, will require high levels of concentration and mental energy. For units operating even semi-autonomous systems from the battlefield, huge amounts of data, requirements for decisions, and self-protection responsibilities will pose major cognitive challenges. At the same time, physical exertion, sleep deprivation, and the psychological stressors of battlefield operations, including uncertainty and the potential for injury or death, will layer over this to only enhance challenges.

While mental energy is often used colloquially, studies suggest that this is a real concept. The vigilance decrement (*vigilance* is the scientific term for sustained attention) and decision fatigue are well-documented phenomena whereby humans lose effectiveness at paying attention and making complicated decisions over time in taxing situations. In a recent Air Force study, researchers asked Servicemembers to perform a task that required them to monitor a computer screen to identify whether small icons representing planes were flying toward or away from each other. Compared to the first 10-minute period, accuracy fell approximately 5 percent for each additional 10 minutes on task until it ended at 40 minutes—with the individuals at only 85 percent performance.[8] This is mirrored in today's operational force. Despite piloting the aircraft from air conditioned rooms in the United States, today's unmanned aerial vehicle operators can only operate for a limited amount of time before taking a break to recover mentally.

Thus, while analytical systems, decision-support software, and other cognitive aids will help humans, this picture of future operations suggests that they will strain human capabilities; however, another set of emerging technologies has the potential to improve the ability of humans instead of simply helping us use our existing capabilities. Proven and emerging technologies in the field of human performance modification have the potential to enhance the military performance of personnel on the future battlefield. The U.S. military has used stimulants, such as amphetamine "go pills" and newer versions such as the cognitive stimulant modafinil for decades, but new technologies show the potential for more targeted and varied enhancement.

Returning to the Air Force study on vigilance, the group whose mental performance declined with time was the control group. Two other groups used a technology called transcranial direct-current stimulation (tDCS), which is widely used in academic laboratories and to date has a clean safety profile. tDCS passes a weak electrical current through the skull using electrodes taped to the forehead. The electrical current changes how easy it is for nerve cells in the brain to fire. In the Air Force study, tDCS positioned over areas of the brain involved in attention enabled the personnel to focus with no dip in performance throughout the whole 40-minute study. In other studies, researchers have demonstrated that tDCS can enhance the speed of learning (including in militarily relevant tasks, such as radar returns) and improve threat detection.

tDCS is only one of a range of technologies that show the potential to enhance human performance. For example, research taking place in the U.S. military and in academia has identified hormones and neurotransmitters in the blood that are associated with the ability of special operators to perform at high levels despite extraordinary physical and mental demands and highly stressful environments.[9] If the relationship is causal, this research suggests a potential route through which performance could be enhanced or maintained over long missions.

Returning to the NeXTech wargames, the organizers specifically tasked one group with examining applications of human performance modification technologies. Commensurate with this article's vision of the human role in future warfare, participants did not focus primarily on traditional types of physical enhancement. Rather, to improve the

Lexus RX450h retrofitted by Google for its driverless car fleet parked near Tesla Model S electric car (Steve Jurvetson)

ability of a hypothetical American force, participants were most interested in enhancing cognitive traits. They wanted more perceptive individuals with the ability to stay clear headed under stress and who needed minimal sleep to operate at high levels of effectiveness.

This vision of the future soldier is far from the berserkers of many science fiction depictions, and participants had good reason to steer away from old conceptions of super soldiers; in most cases, they would be counterproductive from the U.S. point of view. Indiscriminate killing would go against both the laws of war and good tactics and operational art, as local populaces often play an important role in achieving long-term objectives. The value of performance enhancement technologies will only be emphasized by the fact that each Soldier, Marine, Sailor, and Airman is likely to play an even more important role in future conflicts. To destroy a target in World War II took thousands of individuals manning hundreds of bombers. Today, one pilot can achieve the same destruction. Tomorrow, one individual may control tens or hundreds of partially autonomous systems.

While this technology area has substantial promise, there are important ethical questions surrounding military use, many of which are summarized in a report by Dr. Patrick Lin of the California Polytechnic State University.[10] A key factor is that demonstrating the effectiveness of human performance technologies in military environments will require testing in military populations. At the same time, governments, including the U.S. military, have historical records of conducting unethical research, especially for national security purposes. Even today with strict controls in place, conducting ethical research in military environments is challenging because the chain of command is inherently—and necessarily—coercive (military personnel must follow orders for the system to function properly). Informed consent is the cornerstone of modern research ethics, but this environment makes it difficult to separate true consent from the influence of the chain of command, although ongoing research overseen by review boards shows that it is possible to gain true informed consent. There is also the possibility that enhancements inadvertently harm individuals, affect others' perceptions of those who take them, give some individuals a leg up on others, and may affect reintegration into society. These are important questions deserving of careful consideration, but likewise, we should also ask whether we have an obligation to provide enhancements that make our military

personnel less likely to be injured or killed on the battlefield.

These and other issues will affect interest in performance enhancers and the willingness of DOD to provide them to military personnel. While analyzing these issues, we must also be cognizant of the fact that from the individual military operator's point of view, there is substantial interest. In a recent survey of Army personnel, more than 50 percent take supplements weekly, and based on 5 years of discussions with military personnel on the topic, I can say comfortably that interest in performance enhancement is very high.[11] Nonetheless—and somewhat ironically—the same ethical factors that are likely to keep humans on the battlefield will also push some countries to limit the ways in which they enhance warfighters' capabilities.

Not all actors abide by the same ethical boundaries, though, so this is also an area of potential asymmetry going forward. Nonstate actors, especially terrorist groups, may have the least compunction about using these technologies. If an organization is willing to conduct suicide attacks, then it probably would not care about long-term damage from an enhancement: news reports suggest that the terrorists who carried out the 2008 attacks in Mumbai used stimulants such as cocaine to stay up for long periods of time.[12]

Stepping Back

A confluence of technical, tactical, operational, strategic, and ethical reasons strongly suggests that humans will still play crucial roles in all aspects of warfare over the next two decades—and probably much longer. As highlighted above, we must be vigilant for nonlinear advancements in science and technology that could change the way states and other actors conduct military operations. But we should also be cognizant of the emerging tools to enhance human-computer interactions and human performance directly, which may shift the balance even more toward humans. The interactions between humans, human-computer teams, and autonomous systems on the battlefield of the future and how to optimize these are little-studied areas, but as the TOPGUN and other examples above demonstrate, we must work to find the right balance because it will likely provide a considerable advantage—and when we find this balance, human performance will continue to drive a large part of military effectiveness. **JFQ**

Notes

[1] Joe Braddock and Ralph Chatham, *Report of the Defense Science Board Task Force on Training Superiority & Training Surprise* (Washington, DC: Defense Science Board, January 2001), available at <www.acq.osd.mil/dsb/reports/ADA386579.pdf>.

[2] Adam Fisher, "Google's Road Map to Global Domination," *The New York Times*, December 11, 2013, sec. Magazine, available at <www.nytimes.com/2013/12/15/magazine/googles-plan-for-global-domination-dont-ask-why-ask-where.html>.

[3] A. Paul Alivisatos et al., "The Brain Activity Map Project and the Challenge of Functional Connectomics," *Neuron* 74, no. 6 (June 2012), 970–974.

[4] Gary Kasparov, "The Chess Master and the Computer," *The New York Review of Books*, February 11, 2010, available at <www.nybooks.com/articles/archives/2010/feb/11/the-chess-master-and-the-computer/>.

[5] Stuart Fox, "Insurgents Hack Predator Video Feed With $26 Software," *Popular Science*, December 17, 2009, available at <www.popsci.com/technology/article/2009-12/insurgents-hack-predator-video-feed-26-software>.

[6] Pavel Aksenov, "The Man Who May Have Saved the World," *BBC News*, September 26, 2013, available at <www.bbc.co.uk/news/world-europe-24280831>.

[7] Department of Defense Directive 3000.09, "Autonomy in Weapon Systems," November 21, 2012, available at <http://fas.org/irp/doddir/dod/d3000_09.pdf>.

[8] Jeremy T. Nelson et al., "Enhancing Vigilance in Operators with Prefrontal Cortex Transcranial Direct Current Stimulation (tDCS)," *NeuroImage* 85, part 3 (January 15, 2014), 909–917.

[9] Charles A. Morgan et al., "Relationships among Plasma Dehydroepiandrosterone Sulfate and Cortisollevels, Symptoms of Dissociation, and Objective Performance in Humans Exposed to Acute Stress," *Archives of General Psychiatry* 61, no. 8 (August 2004), 819–825; and Charles A. Morgan et al., "Relationship among Plasma Cortisol, Catecholamines, Neuropeptide Y, and Human Performance during Exposure to Uncontrollable Stress," *Psychosomatic Medicine* 63, no. 3 (2001), 412–422.

[10] Patrick Lin, Maxwell J. Mehlman, and Keith Abney, *Enhanced Warfighters: Risk, Ethics, and Policy* (New York: The Greenwall Foundation, January 1, 2013), available at <http://ethics.calpoly.edu/Greenwall_report.pdf>.

[11] Harris R. Lieberman et al., "Use of Dietary Supplements among Active-Duty U.S. Army Soldiers," *The American Journal of Clinical Nutrition* 92, no. 4 (October 1, 2010), 985–995.

[12] Damien McElroy, "Mumbai Attacks: Terrorists Took Cocaine to Stay Awake during Assault," *The Telegraph* (London), December 2, 2008, available at <www.telegraph.co.uk/news/worldnews/asia/india/3540964/Mumbai-attacks-Terrorists-took-cocaine-to-stay-awake-during-assault.html>.

Airman refuels F-15 Eagle aircraft attached to 125th Fighter Wing during exercise Vigilant Shield 15 (U.S. Air Force/Brandon Shapiro)

DOD Response Under the Stafford Act

A Call to Action

By Richard J. Hayes, Jr.

Hurricane Katrina revealed our nation's lack of preparedness to respond to a complex catastrophe in a rapid, efficient, and effective manner.[1] This catastrophe forced a reevaluation of how we plan for and respond to natural disasters and/or emergencies. Over the last 10 years, efforts have focused on new response frameworks and building capacity to respond to such events, but little consideration has been given to capitalizing on a process that would rapidly generate and deploy Title 10 Department of Defense (DOD) capabilities, especially the Reserve components. DOD needs to revise processes in the Adaptive Planning and Execution System (APEX) to recognize and capitalize on the inherent advantage of using Reserve forces in closest proximity to incidents. The current process is cumbersome, inefficient, and potentially leads to unnecessary loss of life and human suffering. History has illustrated over and over again that the first 72 hours of any catastrophe is the window in which we are most likely to save lives. Squandering time to run mobilization of Reserve units through the current force generation process is unacceptable.

Brigadier General Richard J. Hayes, Jr., USA, is Assistant Adjutant General–Army and Director of the Joint Staff, Illinois National Guard.

Recent Catastrophes

The National Guard (NG), constitutionally under the command and control of the governors of the states and territories, has a primary role to support civilian authorities in the aftermath of emergencies and disasters. The NG has always been the most responsive military asset aligned to perform this role due to the close proximity of the units situated in more than 3,000 communities throughout the Nation. In 2012, Congress wisely expanded community-sourced capabilities with a change to Title 10 U.S. Code (USC)

§ 12304(a) contained in the 2012 National Defense Authorization Act (NDAA).[2] Today, governors finally have the means to access the Reserve components of the military Services to support a response under The Robert T. Stafford Disaster Relief and Emergency Assistance Act, as Amended.[3]

Katrina clearly illustrated that the Active component (AC) and, more important, the NG can rapidly muster and deploy tens of thousands of personnel with a vast array of capabilities, often within the first 12 to 72 hours. The Reserves of the Army, Marines, Navy, and Air Force were not included as part of response efforts for Hurricane Katrina. While accessing the Reserves is a reality today, DOD's sourcing process is cumbersome and has not captured the intent of the 2012 NDAA in which Congress recognized the responsiveness of the Reserves for these types of events. Like the NG, the Reserves are located in communities throughout the country.

Furthering the knowledge captured from lessons learned with Hurricane Katrina, National Level Exercise 2011 studied a complex catastrophe along the New Madrid Fault involving a future multistate earthquake in the Midwest. The after-action report revealed that a response to a 7.7 magnitude earthquake was likely complicated due to numerous cascading effects outside the zone of impact. The predicted Defense Support of Civil Authorities (DSCA) required is expected to be on a scale not seen in any previous disasters/catastrophes.[4] It is well known that state and local governments cannot afford to fund significant contingency capabilities; they rely on mutual aid agreements, compacts, and mutually supportive response frameworks to come to each other's aid when local incident response resources are exhausted. When we compare state and local contingency capacity to that of the entire U.S. defense establishment, it is clear that the defense establishment's depth is unmatched and specifically funded to train for and execute contingency operations in either a homeland defense or homeland security role (up to and including response to emergencies, disasters, and complex catastrophes).

Federal and State Responsibilities and the Constitution

The states have the primary responsibility both for homeland security and for response to emergencies, disasters, and complex catastrophes. A key legal exception to this is codified under the Insurrection Act of 1807, which grants the President special powers relating to a state's inability to enforce its own and Federal law. The U.S. Constitution established the rights of the people and delineated the rights and responsibilities between the several states and the Federal Government. The Preamble to the Constitution states, "We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity."[5]

The Constitution affirms common (homeland) defense as a primary Federal responsibility:[6] The "United States . . . shall protect each [state] of them against invasion; and . . . against domestic violence."[7] The term *domestic violence* relates to powers granted to the President under the Insurrection Act.[8] The Second Amendment recognizes the rights of the several states to form and have "a well regulated Militia, being necessary to the security of a free State,"[9] and the Tenth Amendment provides that "powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."[10] These key provisions place primary responsibility for homeland security and the general welfare of the people with the states and territories, and defense of the homeland with the Federal Government, specifically, the Department of Defense. Governors inherently are the heads of state and therefore are ultimately responsible for the security and general welfare of the people in their geographic jurisdictions. The importance of the Constitution in this discussion is that all disasters are state matters; therefore, state and local governments, when able to act in this capacity, are always in charge of their response. The Federal Government solely supports these efforts.

The Stafford Act provides the legal authority for the Federal Government, including DOD, to provide assistance to the states in cases of emergencies or natural and other disasters outside of Immediate Response Authority (IRA).[11] Under the Stafford Act, the President is delegated emergency powers and may declare an event a major disaster or emergency. Generally, Stafford Act assistance is provided upon request of a governor, provided certain conditions are met: primarily, the governor must certify that the state lacks the resources and capabilities to manage the disaster or emergency. The Stafford Act allows the President, on his own authority, "to declare an emergency, but not a major disaster . . . with respect to an emergency that 'involves a subject area for which, under the Constitution or laws of the United States, the United States exercises exclusive or preeminent responsibility and authority.'"[12] "A prime example of preeminent federal authority . . . lies in the realm of homeland defense."[13] For a detailed discussion of the roles of the states and the Federal Government under the Stafford Act, please read the *Domestic Operational Law Handbook*.[14]

Lessons Learned from Hurricane Katrina

Hurricane Katrina marked a new era for the emergency management field and gave birth to a whole host of efforts in developing revised strategies, new frameworks, and plans, and was a precursor to the DOD concept of a complex catastrophe.[15] A 2006 Government Accountability Office (GAO) report to Congress revealed that key failures in responding to Katrina were from a lack of a framework outlining leadership roles, responsibilities, and lines of authority at all levels, and the failure to clearly define and communicate the same to facilitate rapid and effective decisionmaking.[16] The report also highlighted the lack of detailed plans needed to delineate capabilities that might be required, and how to

Federal civil authorities supported by DOD respond to simulated 6.0 magnitude earthquake on New Madrid Fault Line as part of National Level Exercise 2011 (U.S. Air Force/Maxwell Rechel)

provide and coordinate such assistance.[17] Prior to Katrina, the typical Federal posture was to wait for the affected states to request assistance.[18] Katrina illustrated how the NG and AC could muster tens of thousands of personnel with a vast array of capabilities within the first 72 hours.

Friction Among the States and Federal Government

In response to Hurricane Katrina, 54,000 NG and 20,000 Title 10 personnel were deployed to the Gulf Coast under separate chains of command.[19] The difficulties in integrating Servicemembers under separate chains led President George W. Bush to ask the governors of the three states involved to appoint Lieutenant General Russel L. Honoré as a dual-status commander and place all forces under his command, effectively Federalizing the NG. All three governors refused, including the President's brother, Governor Jeb Bush of Florida.[20]

After Katrina, the DOD solution was to have command and control over all military forces in domestic (and, in particular, multistate) emergencies, including NG forces.[21] DOD proposed legislation that became part of the 2007 NDAA. The 2007 NDAA amended the Insurrection Act of 1807, which for 1 year allowed the President, without the prior knowledge or consent of the governors, "to federalize the National Guard and mobilize all other military components to respond to *'any serious emergency.*'"[22]

In reaction to this in 2007, the Commission on the National Guard and the Reserves and the Council of State Governments called for the repeal of the changes to the Insurrection Act, which was accomplished in the 2008 NDAA.[23] DOD proposed similar legislation in 2009 and 2010 that did not pass.[24] In 2010, President Barack Obama established the Council of Governors (COG) by executive order.[25] In consultation with DOD, the COG developed the Joint Action Plan for "Developing Unity of Effort."[26] The Joint Action Plan provides that:

the Governor of the State affected will normally be the principal civil authority supported by the primary federal agency and its supporting entities and the Adjutant General of the State or his/her subordinate designee will be the principal military authority supported by a duly appointed Dual-Status commander acting in his or her State capacity.

In the 2012 NDAA, Congress incorporated these principles into Federal law.[27]

The 2012 NDAA also expanded Federal assistance under the Stafford Act by providing the Secretary of Defense the authority to order members of the Reserves to Active duty for up to 120 days "to respond to the Governor's request."[28]

Strategic Plans and Policy Guidance

Currently, the Office of the Secretary of Defense's 2012 Guidance for Employment of the Force only recognizes the primacy of the NG of the states and territories, acting under state control, to provide initial response forces for natural or manmade catastrophes with the only prime exception related to the chemical, biological, radiological, nuclear, and explosives response enterprise.

The 2013 *Strategy for Homeland Defense and Defense Support of Civil Authorities* highlighted that "defending U.S. territory and the people of the United States is the highest priority of the Department of Defense, and providing appropriate defense support of civil authorities is one of DOD's primary missions."[29] Part of this strategy recognizes leveraging IRA,[30] geographic proximate force sourcing, and ready access to non–National Guard Reserve forces.[31] While this groundbreaking strategy offers a proper focus to the topic, little if any changes were offered in the 2014 Quadrennial Defense Review[32] and the DOD fiscal year 2015 budget request[33] to ensure this reality is achieved; this highlights the disconnect between current strategy and policy.

State Approaches

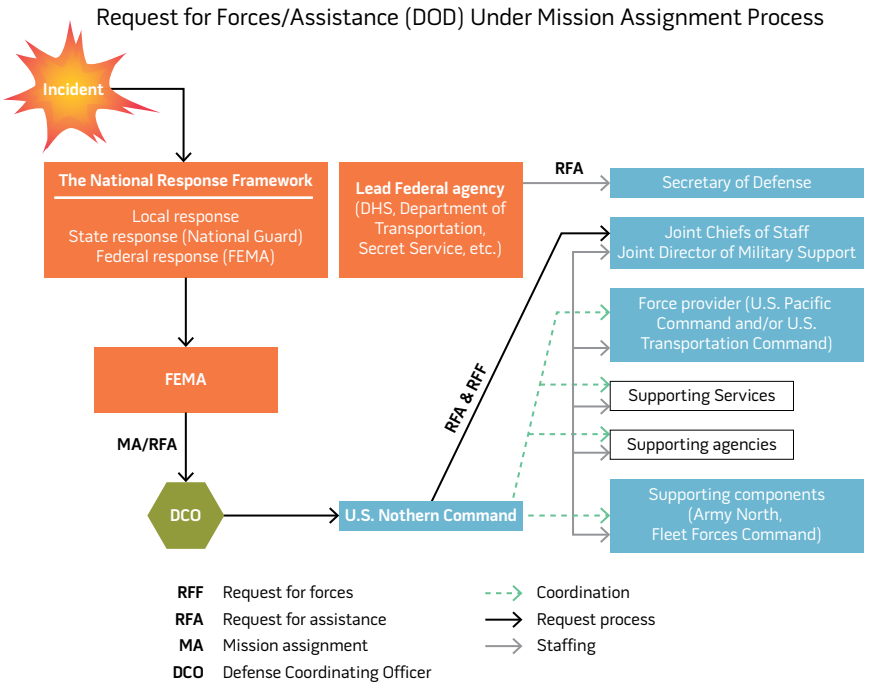
Historically, when preparing for disasters, state emergency management agencies (EMAs) and the states' National Guard units work with local partners to network, establish relationships within the National Response Framework, and develop all hazard response plans maximizing mutual aid between civilian agencies and the NG. In addition, many states have operation plans to respond to known potential catastrophes along key terrain. Today, the rest of DOD is largely not engaged in these discussions at the state and local levels with exception to the Defense Coordinating Elements located in each of the 10 Federal Emergency Management Agency (FEMA) regions.[34]

Where capabilities exceed capacity, planned or not, local mutual aid agreements and state-to-state Emergency Management Assistance Compacts (EMACs) have been the typical means to fill shortfalls. When they are not adequate in terms of capabilities or time available to employ them, requests for Federal assistance are made. State National Guards primarily receive mission assignments from their respective state EMAs. These mission assignments can be under Title 32 under IRA or, if requested outside of IRA, under state Active duty or Title 32 § 502(f) if authorized by the Secretary of Defense under a Stafford Act declaration.[35]

Sourcing of Military Capabilities by the States

For a state to secure Title 32 forces located outside its borders, state-to-state EMAC requests for NG forces have been the typical arrangement to obtain needed military capabilities.

Figure 1. DOD Sourcing Process for DSCA



Outside of IRA, Title 10 forces are typically deployed only after the President declares a Federal emergency or disaster under the Stafford Act or Insurrection Act.

When a state governor requests a Federal capability, FEMA, under the Department of Homeland Security, becomes the lead agency for managing such requests under a Federal response declared under the Stafford Act. With a Stafford Act declaration, FEMA will typically establish a joint field office (JFO) comprised of a state coordinating officer, Federal coordinating officer, and Defense coordinating officer (DCO), along with their supporting staffs.

Predicated that all state assets are exhausted, including the state's National Guard, the state EMA will generate a mission request for a capability and then either pass it to another state under EMAC or send it to the JFO to source the capability from assets nested in the Federal Government. If the request is determined to be a Title 10 solution, the DCO validates the request and forwards it to U.S. Northern Command (USNORTHCOM) for sourcing and generation using the Joint Operation

Water purification specialist, part of unit deployed into Rockaway, New York, in direct support of FEMA, state, and local officials, channels water away from housing complex after Hurricane Sandy (U.S. Army/John Adams)

Planning and Execution System (JOPES) as outlined in figure 1.[36]

The Title 10 capability, once approved by the Secretary of Defense, deploys and comes uner the operational control of USNORTHCOM. The usual and customary command and control arrangement in support of civil authorities, including major disasters and emergencies, is through the establishment of a dual-status commander (a National Guard officer of the state) trained and qualified by the USNORTHCOM commander. The governor of the affected state will request that the President approve the activation of a dual-status commander.[37] The USNORTHCOM commander will assign the dual-status commander either operational or tactical control of Title 10 forces.

The process for generating and deploying Title 10 forces under this current system is not as responsive as the one used by the NG; JOPES was largely designed to handle defense of the homeland and to fight the Nation's wars. The NG excels at rolling out the door at a moment's notice at the governor's request in large part because they live within 50 miles of the units they serve and the process for employment is streamlined.

Congress recognized the same inherent potential with the Reserves when Congress changed 10 USC § 12304(a) in the 2012 NDAA; clearly Congress envisioned the Reserves of the military Services as having the ability to be equally responsive as the NG.

There has been much discussion on this topic. In discussion with many of the DCOs, there is an overriding concern that the Reserves are too expensive and the AC is more cost effective because pay and allowances are already expensed in the base DOD budget; the only additional cost for AC forces is related to transporting and sustaining the Title 10 force deployed. While this statement is true, it does not take into consideration the importance of generating forces within the first 12 to 72 hours when the greatest opportunity to save lives is probable. Incident commanders focus on solving the problems that confront them and they really do not care about where a capability comes from—they are solely concerned that the capability gets there quickly.

Like the NG, Reserve units are present in every state and in over 3,000 communities across the country. AC Title 10 forces, on the contrary, are more concentrated and geographically constrained, hindering the response time due to proximity necessary to assist with the aftermath of an emergency or catastrophe; APEX for these purposes currently lacks speed and efficiency. The AC also does not dedicate training time or resources to be able to respond under the National Incident Management System.[38]

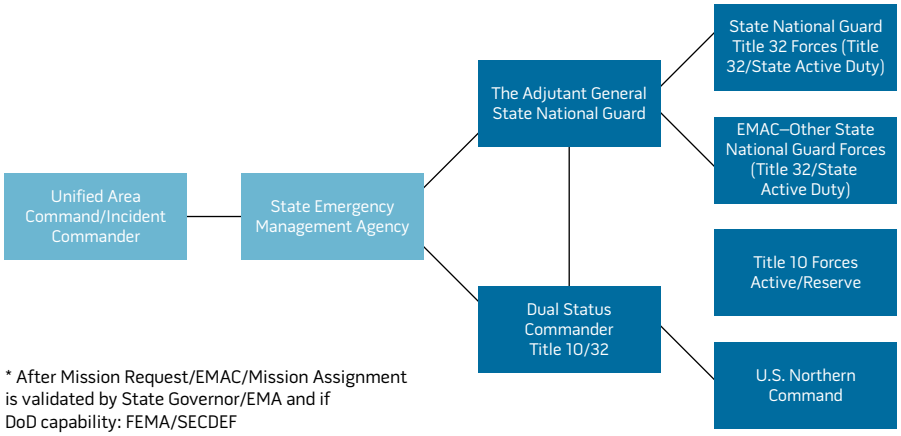
In contrast, state NGs are much more responsive to another state's requests for assistance under EMAC. Figure 2 highlights the usual and customary flow that military capabilities can expect to follow once issued a mission assignment under an EMAC or request emanating from the DCO. It is crucial to recognize that the NG construct involves two phone calls followed by a written request, whereas the Title 10 request process has to circulate through much of DOD. The Defense Department needs to look at the sourcing process from the incident commander's perspective. One complicating factor not experienced to date is the resource adjudication process associated with a complex catastrophe as it relates to state-to-state EMACs.[39]

The Reserves can generate and deploy capabilities from the very communities they live in as rapidly as the NG if DOD changes the current process used to source them. Like the NG, Reserve members are members of the communities and states in which they live and have the opportunity to be integrated in the response plans of the state's EMAs. They also have an inherent care for the citizens in the states they serve in. Hurricane Sandy illustrated the seamless integration of all military components in their response under a dual-status commander construct. The only difference was Sandy was forecasted days before it occurred. What would happen with a truly no-notice event like a catastrophe (for example, an earthquake) along the New Madrid Fault?

DOD needs to attack this problem from three fronts. One, direct the commanders of the Reserve components to have their subordinate commands establish relationships with the state EMAs and NGs in the states in which their units reside; assign all units a core mission assignment in line with the NG Core 10 capabilities as outlined in National Guard Regulation 500-1.[40] Two, the DCOs working in conjunction with USNORTHCOM should track and monitor Active and Reserve unit capabilities and readiness cycles to know which units are ready to deploy rapidly at the request of a governor. It is acknowledged that individual Servicemember readiness standards for fitness for duty will drive deployment of any individual but that should not stop the entire unit from deploying. Three, DOD needs to establish new policies and regulations to address sourcing of Reserve assets and consider delegating force generation to the commander of USNORTHCOM, executing mobilization in conjunction with the Services and DCOs.

Figure 2. Typical Force Flow for DSCA

Usual and Customary Flow of DOD Assets to Incident Under Mission Assignment Process*



* After Mission Request/EMAC/Mission Assignment is validated by State Governor/EMA and if DoD capability: FEMA/SECDEF

Conclusion

DOD has not implemented a process to exploit the use of the Reserves in response to requests from a governor for support under the Stafford Act nor has it embraced the 2013 *Strategy for Homeland Defense and Defense Support of Civil Authorities*. The Defense Department needs to fully adopt this 2013 strategy through revision of the Guidance for Employment of the Force, policies relating to DSCA, and processes to generate and deploy forces under the Stafford Act. U.S. citizens see our military through one lens and are only interested that their military arrives ready to assist in a rapid, efficient, and coordinated manner in a time of need. JFQ

Notes

[1] Secretary of Defense Leon Panetta, "Memorandum for Secretaries of the Military Departments," July 20, 2012. The term *complex catastrophe* is solely a Department of Defense (DOD) term.

[2] National Defense Authorization Act (NDAA) for Fiscal Year 2012, 112th Cong., Pub. L. 112-81, div. A, title V, § 515(a)(1), December 31, 2011; 10 USC 12304(a), available at <www.gpo.gov/fdsys/pkg/PLAW-112publ81/html/PLAW-112publ81.htm>.

[3] The Robert T. Stafford Disaster Relief and Emergency Assistance Act, as Amended, April 2013 (the Stafford Act), available at <www.fema.gov/media-library-data/1383153669955-21f970b19e8e-aa67087b7da9f4af706e/stafford_act_booklet_042213_508e.pdf>.

[4] Government Accountability Office (GAO), *Actions Are Needed to Improve DOD's Planning for a Complex Catastrophe*, GAO Report 13-763 (Washington, DC: GAO, September 30, 2013), 2.

[5] The Constitution of the United States, preamble, available at <www.senate.gov/civics/constitution_item/constitution.htm>. Emphasis added.

[6] Ibid.

[7] Ibid.

[8] Ibid. The Insurrection Act of 1807 is the statutory implementation of Congress's authority under Article 1, § 8 of the U.S. Constitution to "provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrection and repel Invasions. . . ."; it is also known as the Militia Clause.

[9] Ibid.

[10] Ibid.

[11] Dave Sherry and Robert Pirone, eds., *2013 Domestic Operational Law Handbook: A Practitioner's Guide for Judge Advocates*, Center for Law and Military Operations (CLAMO), The Judge Advocate General's Legal Center and School (Charlottesville, VA: CLAMO, October 2013), 29.

[12] Ibid., 33.

[13] Paul Stockton, "DOD and the Problem of Mega-Catastrophes," Center for International Security, Stanford University, in *Threats at Our Threshold: Homeland Defense*

Deputy Secretary of Defense addresses attendees during APEX Senior Executive Orientation Program designed to provide joint orientation for new executives in DOD (DOD/Adrian Cadiz)

and Homeland Security in the New Century, ed. Bert B. Tussing (Carlisle, PA: U.S. Army War College, 2006), 24, available at <http://csis.org/images/stories/HomelandSecurity/071022_Chap1Mega-Catastrophes.pdf>; Stockton's paper introduces the friction a large-scale complex catastrophe may cause as it relates to Federal response under the Stafford Act and possible application in complex catastrophes.

[14] Sherry and Pirone.

[15] National Level Exercise 2011 reviewed the aftermath of a 7.7 magnitude earthquake along the New Madrid Fault.

[16] GAO, *Statement by Comptroller General David M. Walker on GAO's Preliminary Observations Regarding Preparedness and Response to Hurricanes Katrina and Rita*, GAO Report GAO-06-365R (Washington, DC: GAO, February 2006), 3.

[17] Ibid., 5.

[18] Ibid., 4.

[19] Ludwig J. Schumacher, "Dual Status Command for No-Notice Events: Integrating the Military Response to Domestic Disasters," *Homeland Security Affairs* 7, no. 4 (February 2011), 2.

[20] Ibid.

[21] Ibid.

[22] Ibid. Emphasis added.

[23] Ibid., 2–3; see also "The Council of State Governments: Resolution in Support of the Governors' Power to Control the National Guard," June 13, 2007.

[24] Ibid., 3–4.

[25] Schumacher.

[26] National Governors Association Council of Governors, "Joint Action Plan for Developing Unity of Effort," available at <www.nga.org/files/live/sites/NGA/files/pdf/CoGPlanforDevelopingUnity.pdf>.

[27] NDAA for Fiscal Year 2012, Pub. L. 112-81, § 515(c); 32 USC 317.

[28] NDAA for Fiscal Year 2012, Pub. L. 112-81, § 515(a); 10 USC 12304(a).

[29] *Strategy for Homeland Defense and Defense Support of Civil Authorities* (Washington, DC: Office of the Assistant Secretary of Defense, February 2013), 1.

[30] DOD Directive 3025.18 grants Federal military commanders and/or responsible DOD civilian officials to act from a request by a competent civilian authority to save lives, prevent human suffering, or mitigate great property damage within the United States. This DOD Directive is also known as Immediate Response Authority.

[31] Ibid., 17.

[32] Secretary of Defense, *Quadrennial Defense Review* (Washington, DC: Office of the Secretary of Defense, March 4, 2014).

[33] DOD, "Fiscal Year 2015 Budget Request," March 2014, available at <www.defense.gov>.

[34] GAO, *Actions Are Needed*, 39.

[35] Required Drills and Field Exercises, Title 32 USC § 502(f), available at <www.law.cornell.edu/uscode/text/32/502>. Title 32 forces are under the command and control of the governor of the state in which they reside.

[36] GAO, *DOD Can Enhance Efforts to Identify Capabilities to Support Civil Authorities during Disasters*, GAO Report GAO-10-386 (Washington, DC: GAO, March 2010), 39; the Joint Operation Planning and Execution System is also known as the Adaptive Planning and Execution System.

[37] GAO, *Actions Are Needed*, 9.

[38] David Theisen, "DOD Support of Civil Authorities during No-Notice Complex Catastrophes," Master's thesis (Carlisle, PA: U.S. Army War College, March 2013), 1.

[39] Emergency Management Assistance Compact (EMAC), "Mutual Aid History," available at <www.emacweb.org/index.php/learnaboutemac/history/mutual-aid-history>. Established in 1996, EMAC stands today as the cornerstone of the Nation's mutual aid system. EMAC is a "first in, first out" system and inherently does not have a formal resource adjudication process.

[40] National Guard Bureau (NGB), *National Guard Domestic Operations*, NGR 500-1 (Arlington, VA: NGB, June 2008), available at <www.ngbpdc.ngb.army.mil>.

U.S. and Korean ships transit Pacific Ocean in 13-ship formation led by USS *Tucson* during exercise Invincible Spirit, July 2010 (U.S. Navy/Adam K. Thomas)

After the First Shots

Managing Escalation in Northeast Asia

By Vincent A. Manzo

The United States has never fought a conventional war against a nuclear-armed adversary. Yet the United States and its allies must prepare for a range of military contingencies with both North Korea and China, and avoiding nuclear escalation would be a U.S. objective in all of them. Developing strategies for managing escalation will be an essential part of U.S. efforts to extend deterrence and assure its allies in Northeast Asia.

Thomas Schelling's writing on coercion and competitions in risk-taking remains valuable for analyzing the challenges associated with escalation management. A U.S. strategy for managing escalation under the nuclear shadow must compel an adversary to stop fighting while demonstrating restraint in U.S. goals and use of force—in other words, withholding punishment—to induce comparable restraint from the adversary. Madelyn Creedon, the former Assistant Secretary of Defense for Global Strategic Affairs, explained the relationship between reciprocal restraint, deterrence, and escalation management: "There is . . . an element of restraint in our reactions [to

Vincent A. Manzo is a Fellow in the Defense and National Security Group of the Center for Strategic and International Studies. He is currently serving as an Intergovernmental Personnel Act Fellow in the Office of the Under Secretary of Defense for Policy.

Kim Jong-un sitting at desk in what appears a dedicated military operations room (Korean Central News Agency)

attacks] as well that is a part of deterrence. Our restraint comes with a promise of more action if there is a response."[1]

This article applies that framework to U.S. military strategy in Northeast Asia. The first section summarizes developments in North Korean and Chinese strategic postures and the implications for U.S. defense strategy. The second part describes Schelling's concept of a competition in risk-taking and argues that it is a valuable framework for developing a strategy for managing escalation. The third section applies this framework to the Korean Peninsula. The final two parts apply the framework to a U.S.-China conventional conflict: the fourth section explores both deliberate and inadvertent escalation risks in such a conflict, and the fifth section discusses several measures for preventing inadvertent escalation.

U.S.–Republic of Korea (ROK) alliance efforts to coordinate a coherent strategy for managing escalation in confrontations with North Korea have made progress. Looking forward, ongoing challenges include identifying developments in a confrontation that would necessitate a shift in objectives from managing escalation to damage limitation or regime change, and determining the role of ROK conventional strike forces and how these capabilities would fit into the alliance's understanding of escalation.

Effective escalation management in a conventional conflict with China would require comparable understandings of escalation between U.S. and Chinese officials, the ability to avoid crossing key thresholds and convey to each other what limits are expected in return, and clear expectations about the consequences of escalation. Because even lower end conflicts would pose profound risks of inadvertent escalation, this article explores U.S. measures for reinforcing mutual restraint in the early phase of a confrontation, but these measures would quickly become infeasible if China did not reciprocate.

The analysis in this article includes two intentional simplifications. The discussion of the Korean Peninsula focuses exclusively on U.S.-ROK efforts to manage escalation in crises and does not address the role of China or Japan. For the U.S.-China section, the discussion explores escalation between the United States and China, but a more comprehensive analysis must also include intentions and actions of other countries involved in a serious U.S.-China crisis, such as Japan or Taiwan. Narrowing the

cast of characters hopefully illuminates fundamental issues, questions, and recommendations that more comprehensive studies can examine further.

Evolving Military Capabilities in Northeast Asia

Both China and North Korea are altering their strategic-military postures. Bradley Roberts, former Deputy Assistant Secretary of Defense for Nuclear and Missile Defense Policy, frames these challenges through two concepts: decoupling and the stability-instability paradox. U.S. allies are concerned that Chinese and, in the future, North Korean capability to strike the U.S. homeland with nuclear missiles could decouple them from U.S. security commitments. And North Korea or China could feel confident that their military capabilities create stable deterrence relationships with the United States, thus empowering them to challenge U.S. allies: North Korea may attempt to coerce and even mount conventional attacks on South Korea and Japan. China might engage in creeping expansionism, gradually asserting control over disputed territory.[2]

A dialogue about the implications of these trends for U.S. defense strategy is already under way.

China has a sophisticated nuclear arsenal and ballistic missile program and is committed to retaining a credible second-strike capability against the United States. For those reasons, several studies have concluded that mutual nuclear vulnerability with China is a fact of life for the United States.[3] China is also deploying a variety of nonnuclear systems, including conventional ballistic missiles for striking bases and aircraft carriers, counterspace weapons for destroying satellites, cyber capabilities for degrading network-dependent systems, attack submarines, integrated air defenses, and aircraft.[4] Many analysts argue that these capabilities support China's antiaccess/area-denial (A2/AD) strategy of defeating U.S. conventional forces in the Western Pacific and preventing additional U.S. forces from entering the region, in part by disrupting U.S. command and control (C2) and intelligence, surveillance, and reconnaissance (ISR) systems.

The Joint Operational Access Concept and the related Air-Sea Battle (ASB) concept are intended to ensure the effectiveness of U.S. conventional forces as China and other countries field A2/AD capabilities. The concepts envision strikes against strategic targets in an adversary's territory early in a conflict. These attacks against C2 and ISR, offensive weapons such as ballistic missiles, and military infrastructure would, if successful, leave the adversary blind, deaf, and dumb in the theater of conflict and much less capable of effective military operations. This would enable the United States and its allies to maintain escalation dominance in a conventional conflict.[5] Yet many analysts argue that this concept underestimates how much China's nuclear posture would constrain U.S. actions in a conventional war. They question whether a President would ever authorize large-scale conventional strikes on mainland China.[6]

The military balance with North Korea is also evolving. The country continues to advance toward an operational capability to deliver nuclear warheads via ballistic missiles. It completed its third nuclear detonation in February 2013, and the U.S. Intelligence Community assesses that it will eventually be capable of miniaturizing nuclear warheads and mounting them on ballistic missiles. A successful satellite launch in December 2012 illustrates progress on the path to developing intercontinental ballistic missiles, while North Korea's current missiles can reach targets in Japan.[7] North Korea also possesses sufficient short-range munitions to devastate Seoul with rapid strikes, which enables it to threaten catastrophic conventional escalation for coercion and deterrence.[8]

Analysts warn that North Korea's emerging nuclear arsenal requires the United States to adjust its plans for conflicts on the Korean Peninsula. North Korean officials would interpret large-scale conventional strikes against high-value political, C2, ISR, and weapons system targets as the start of a campaign to destroy the regime, prompting it to unleash a desperate attempt to end the war through limited nuclear attacks on its neighbors and/or U.S. forces in the region. This development would leave U.S. officials with two horrible options: either continue to fight with conventional means while risking further nuclear attacks, or disarm or destroy the regime and much of the country with nuclear weapons, killing hundreds of thousands of civilians in the process.[9]

The theme running through these critiques is that attempting an early knockout blow could strip away an adversary's incentives for nuclear restraint, and U.S. policymakers might refuse to authorize such operations at the outset of a confrontation. This disconnect could undermine U.S. deterrence. Deterrent threats that are anchored in realistic employment strategies are more credible precisely because the United States might use them. But to be credible, employment plans must acknowledge that escalation concerns would permeate U.S. decisions through every phase of a military confrontation with North Korea and China. As Paul Bracken persuasively argues, managing nuclear risks must be a defining feature of U.S. military strategy in Northeast Asia.[10]

Concepts for Managing Escalation

This reality does not mean the United States should forswear offensive operations against aggressors. Effective and credible extended deterrence and assurance require the United States and its allies to develop effective military options for a variety of contingencies. Otherwise, North Korea or China might see an opportunity to coerce their neighbors while U.S. allies might fear that the emerging military balances with China and/or North Korea could decouple them from U.S. security guarantees.[11] Because of the catastrophic consequences of a limited nuclear exchange, U.S. and allied strategic goals might fall short of total destruction of the adversary's military forces or achieving regime change, at least at the outset of conflicts. Instead, the United States would try to compel the adversary to

stop fighting and restore the status quo while simultaneously deterring it from escalating. Achieving these goals would require both deliberate escalation and establishing mutual limits on the use of force. A coherent strategy for managing escalation would draw upon two related concepts: a competition in risk-taking and deterring escalation.

The goals of employing force in a risk-taking competition are twofold: demonstrate resolve and create a high-risk situation that compels adversary leaders to stop fighting. The magnitude and targets of military operations are calibrated to convince an adversary that the conflict is spiraling out of control, but not to the point where nuclear escalation is a better option than negotiating a peaceful off-ramp. Thomas Schelling described this concept as the threat that leaves something to chance; military actions are extraordinarily dangerous because their consequences are impossible to predict and control. However, employment options tailored to these goals could be compatible with narrower military objectives, such as dislodging forces that recently seized an island. Measured punishment and operations that deny adversary objectives could influence its perceptions about both the costs of escalation and continuing on the current course. From this perspective, deterrence threats do not always succeed or fail in an absolute sense. Threats that do not deter initially can eventually influence an adversary through a process of "progressive fulfillment."[12]

How can an attack impose serious costs and create shared risks yet also convey boundaries on the use of force? The answer lies in the link between reciprocal restraint and deterrence. Every deterrent threat contains a promise of restraint: do not attack us, and we will not attack you. Escalation management requires combatants not to use certain types of weapons and avoid attacks on certain types of targets even after efforts to deter conflict in the first place fail. For example, we will not attack your nuclear weapons as long as you do not use them. To achieve these results, the United States needs to clearly convey that its limited objectives are contingent upon the adversary's willingness to forgo use of nuclear weapons. Delivering this message to adversary leaders in public or private channels would be necessary but not sufficient; U.S. actions must match this message by withholding use of more destructive weapons, limiting the size of an attack, or avoiding certain types of targets, such as C2, political leadership centers, and nuclear forces. Alternatively, deliberately or accidentally ignoring these constraints could precipitate nuclear escalation. Translating this concept into practice requires a sustained effort to understand an adversary's perceptions, values, and strategic goals.[13]

That the United States would need to demonstrate this restraint to its adversary amid the uncertainty, chaos, and mistrust of war poses extraordinary challenges. Misperception, misunderstanding, accidents, faulty intelligence, and inaccurate information could derail efforts to manage escalation. More fundamentally, the United States and its adversary might interpret events differently because escalation is subjective. A 2008 RAND study defined *escalation* as "an increase in the intensity or scope of conflict that crosses thresholds considered significant by one or more of the participants."[14] Two states might observe the same action but interpret its significance differently. One state might cross an adversary's threshold without realizing it. Leaders might not know a threshold exists until it is crossed, or they might not know how they would respond to a provocation until it occurs. Compounding these challenges, the United States would need to balance between resolve and restraint while coordinating its actions with allies, who will have their own goals, concerns, thresholds, and capabilities.

The remainder of this article explores these challenges in the cases of the U.S.-ROK alliance and U.S.-China relations.

Managing Escalation on the Korean Peninsula

Managing escalation in conflicts with North Korea is already a priority for the U.S.-ROK alliance. Following the 2010 Nuclear Posture Review, the alliance began meeting on a regular basis to develop and refine shared strategic concepts for scenarios involving the risk of nuclear escalation. In the words of a South Korean official, the goal of a tabletop exercise at one of these engagements was improving "mutual understanding on responses to nuclear crises."[15] On the operational side, the alliance has agreed upon a counter-provocation plan for small-scale conventional attacks and a tailored deterrence strategy for North Korean nuclear threats. It is also developing a counter-missile strategy and has adopted new guidelines that permit South Korea to deploy longer range conventional ballistic missiles.[16]

Yet questions and challenges remain. The counter-provocation plan is part of alliance efforts to strengthen deterrence of the type of small-scale yet fatal conventional attacks that South Korea suffered in 2010: the sinking of the ROK ship *Cheonan* and the shelling of Yeonpyeong Island. The principal goal of a counter-provocation would be to compel North Korea to stop what it is doing and deter additional attacks without triggering a larger conflict.[17] Unconfirmed articles report that the plan calls for ROK forces to launch an immediate proportionate response against the source of an attack and potentially against one other target, such as forces providing logistical support for the initial provocation.[18]

Confining the military response to targets involved in the attack is a logical approach to preventing escalation. But there is no guarantee that North Koreans would interpret the response in this light. ROK forces involved might conclude that a variety of supporting units were involved in the attack and are thus fair game in the response, resulting in a large retaliatory operation that North Korea could perceive as disproportionate.[19] Another possibility is that North Korean officials authorize a covert provocation to solidify their position against challenges from within the regime. Given those motivations, they might see the consequences of not retaliating against the counter-provocation as more dangerous than escalation.[20] Of course, the alliance must weigh risks that its efforts to manage

escalation might fail against the danger that North Korea's attacks will continue and become more brazen if South Korea forgoes a swift military response. The counter-provocation plan's consultative mechanisms are intended to address situation-specific circumstances that could make responding too dangerous.

Integrating the counter-provocation plan with the alliance's broader strategy for managing escalation, complete with shared concepts, understandings of escalation and alliance options, is an ongoing challenge.[21] What is the line of demarcation between the objectives and options considered under the counter-provocation plan and the ones included in larger military plans to destroy North Korea's conventional and nuclear missiles? Just as importantly, how will U.S. and ROK officials consult over these questions during crises?

Ultimately, U.S. and South Korean perceptions of thresholds, risks, and stakes will vary depending on a variety of situation-specific factors. But U.S. and ROK officials would need to coordinate and execute or forgo employment options in complex scenarios that could escalate quickly, especially if North Korea has operational nuclear missiles and attempts to leverage them for coercion. It is worth remembering that during the Cuban Missile Crisis a handful of governments and news outlets controlled the release of information. Today, North Korea could exploit social media for threats and signaling. Public fears of nuclear escalation might echo through cable news coverage and the blogosphere; rapid dissemination of information and images, accurate or not, could sway domestic opinion either against U.S. involvement or in favor a more drastic response than the President prefers.

For instance, during the spring of 2013, North Korea released a photograph of Kim Jong-un in a command center with large maps depicting missile flight paths to the United States. The state advised diplomats to evacuate and moved ballistic missiles to its coast and mounted them on launchers.[22] Future North Korean attempts at signaling may mirror these displays and include more dangerous actions. As examples, North Korea could detonate a nuclear weapon in the ocean and upload images of the explosion on YouTube, or it might visibly mate nuclear warheads with missiles and deploy them on launch-ready status. How would the alliance respond to small-scale conventional attacks, threats, or demands that occur immediately after these nuclear provocations?

An alliance strategy for escalation management would become increasingly important as South Korea's conventional strike forces evolve. Currently, South Korean declaratory policy is to develop a capability for preemptive conventional strikes against North Korea's nuclear forces. Described as a "missile kill chain," the concept reportedly includes investments in ISR, missile defenses, longer range conventional ballistic missiles, and potential acquisition of air-launched cruise missiles capable of penetrating hardened and buried targets.[23] Beyond technical assessments about the requirements and feasibility of this concept, the alliance would need to address qualitative questions about when to initiate such an employment option, and whether and how the alliance could conduct joint strike operations using both U.S. and ROK capabilities. How would the alliance decide the goal of managing escalation has been overtaken by events and the least bad option remaining is damage limitation?

In theory, this decision is tightly coupled to whether the alliance's overarching objective is regime change or providing Kim Jong-un an off-ramp to save face. Ultimately, U.S. and ROK officials likely will want three types of employment options: options that prioritize managing escalation while the alliance defends itself and seeks a diplomatic end to the war; options for conventional strikes against North Korean nuclear forces; and finally, limited nuclear strike options for achieving the same objective.[24] A unilateral decision by either could leave the United States and South Korea working at cross-purposes, and disagreements about fundamental goals could pull at the seams of the alliance. Fortunately, the alliance has a variety of venues to work through these difficult issues in peacetime.

Deliberate and Inadvertent Escalation with China

Managing escalation with China would be an altogether different challenge. U.S. policy seeks to facilitate greater cooperation with China while tempering military competition through greater transparency, predictability, and eventually common understandings of strategic stability. The emerging competition between China's A2/AD posture and the U.S. ASB concept is one of the most complex challenges these efforts must address. The ASB concept is largely a response to China's A2/AD capabilities, which many U.S. analysts perceive as geared toward providing China with a decisive conventional military advantage over the United States, in part by exploiting U.S. vulnerabilities in space and cyberspace. Interactions between China's A2/AD and U.S. ASB forces could encompass both countries' conventional, space, cyber, missile defense, and nuclear capabilities. In a conventional conflict, both countries would have incentives to coerce the other into making concessions while simultaneously preventing escalation to high-end conventional war and nuclear weapons use.[25] A strategy for managing escalation must understand the risks that stem from these dynamics.

One of the biggest points of contention in debates over ASB is whether a military strategy that relies on striking targets in mainland China with conventional weapons is necessary for effective deterrence or too reckless to be credible. Of course, whether the United States would or should strike the mainland in a specific contingency is impossible to judge in the abstract; the details would matter. Whether the United States should develop conventional strike options is a different question: A credible deterrence posture must at least give the President options to hit targets in the mainland for several reasons. Mainland China would be the staging area from which China would launch conventional missiles at U.S. and allied forces. Purely defensive measures, such as missile defenses and hardening, dispersing, and concealing regional military

South Korean and U.S. admirals inspect wreckage of ROKS *Cheonan* at Pyeongtaek, September 2010 (U.S. Navy/Jared Apollo Burgamy)

assets, would be insufficient as the sole means for coping with China's large conventional strike force.[26] Treating mainland China as a sanctuary could signal that the United States is unwilling to take risks to contest this threat and might reinforce Japanese concerns about decoupling. It could also feed into perceptions among Chinese officials and strategists that they have greater stakes, and thus a decisive advantage, in any conceivable regional conflict.[27]

Moreover, limited conventional strikes on nonnuclear military targets would be consistent with Schelling's concepts of competitions in risk-taking and deterrence through progressive fulfillment. Attacking the homeland of a nuclear power armed with a secure second-strike capability would be an unprecedented action for the United States. It would be a clear sign that the situation is getting out of control. If Chinese strategists previously questioned U.S. commitments, this deliberate decision to escalate could change their calculus and motivate them to seek a peaceful off-ramp.

Although conventional strikes on mainland China would be escalatory by design, they would not inevitably lead to *nuclear* escalation. Elbridge Colby argues that China's investment in an integrated air defense system suggests that it anticipates defending against attacks on the homeland during a conventional war, while the threat of U.S. nuclear retaliation creates strong incentives for China to forgo a nuclear response to a conventional attack. Colby also describes how the United States could reinforce these incentives by tailoring conventional strikes to reflect limited objectives and demonstrate a willingness to show continued restraint and/or withhold punishment: "Logical steps include observing geographic boundaries for such a fight, cordoning off certain kinds of targets [nuclear C2 and weapons; leadership headquarters], and clearly and credibly communicating efforts at limitation to an adversary."[28]

Operationalizing this framework requires U.S. strategists to address several worrisome risks of inadvertent escalation. Could the United States reliably avoid the targets that are off limits during a conventional conflict, and would Chinese officials perceive this as a deliberate act of restraint? Just as importantly, if the United States hit the wrong target by accident or due to flawed intelligence, would Chinese officials see it as an intentional expansion of U.S. war objectives?

One reason for skepticism is that both countries see early attacks on C2 and ISR via conventional weapons, cyber attacks, and counterspace weapons as a means of negating the other's military power. Although this could yield significant military advantages, it could also cause either or both to lose the ability to

communicate clearly and quickly, operate with precision, and assess what is and is not happening on the battlefield. Without reliable C2, deployed forces may take actions that exceed the limits senior officials believe are necessary to induce reciprocal restraint and may fail to receive ceasefire orders. A study of Iraqi decisionmaking during the first Gulf War concluded that a commander decided to burn Iraqi oil fields because he was unable to communicate with his superiors in Baghdad and "feared the worst."[29] In that sense, undercutting China's C2 system could undercut U.S. efforts to manage escalation.

Additionally, space and cyber assets are integral to U.S. and Chinese C2 and ISR systems. Strategists in both countries argue that attacking assets in space and cyberspace would be an effective means of severing links between the other military's sensors, command systems, and deployed forces.[30] Fear of losing C2 and ISR as a result of the adversary's blinding attack, combined with the possibility of gaining a decisive advantage by attacking first, could create pressure for nonnuclear preemptive strikes anytime a military conflict appears likely.[31] Although resilient and redundant systems could dampen this pressure, uncertainty about the capabilities and effects of cyber and counterspace attacks and the absence of clear thresholds in these domains open the door to misperception and miscalculation.[32] Hostilities or misunderstandings in these domains after an accident or incident among U.S., Japanese, and Chinese forces could transform an isolated crisis into a larger military confrontation that none sought.[33]

Blurred nuclear thresholds create additional risks of inadvertent escalation. China deploys both nuclear and conventional variants of its medium-range ballistic missiles, such as the DF-21, and some of its bases, command headquarters, and ground-based sensors might serve both conventional and nuclear operations. The ASB emphasis on achieving both force protection and coercive leverage by suppressing Chinese conventional missiles could translate into large-scale strike operations against a range of targets on the mainland. Yet U.S. forces might struggle to distinguish between nuclear and conventional targets. Chinese officials, in turn, could interpret an inadvertent U.S. strike on a nuclear missile or dual-purpose base or sensor as an attempt to destroy China's nuclear deterrent, especially in light of their concerns about the first-strike potential of U.S. conventional weapons and missile defenses.[34]

Under these circumstances, Chinese strategists may envision limited nuclear strikes against military forces in the region as a last resort option for shocking U.S. officials and compelling them to de-escalate. Whether the Second Artillery Corps has developed such employment options is unclear; it is also unclear whether China's no-first-use policy considers conventional strikes against targets on the mainland as crossing the first-use threshold.[35] Additionally, national decisionmakers in both countries simply do not know how they would react as a conventional conflict escalates.

Deliberate nuclear signaling by both countries before the start of a conventional conflict could exacerbate all of these dynamics. China might disperse its mobile nuclear-armed missiles to signal resolve; however, U.S. officials could interpret these actions as preparation for an attack.[36] Alternatively, U.S. officials could interpret the signal correctly and conclude a strong response is necessary to demonstrate that nuclear threats against the United States are ineffective. Such calculations could prompt the United States to draw attention to its own nuclear capabilities. Yet the preferred means of nuclear signaling for the United States—forward deploying or exercising nuclear-capable bombers—could further blur the nuclear threshold if the United States later employs these types of platforms for conventional strikes on the mainland.[37]

Managing Escalation in Conflicts with China

Given these dangers, U.S. officials may want measures for preventing quick escalation in lower level conflicts. A declaratory and employment policy of early restraint in space and cyberspace would help establish a barrier between an accident or isolated confrontation and a larger conventional conflict. Constraining offensive actions in these domains until the President decides to escalate might be sufficient. U.S. restraint would thus not need to be permanently tied to Chinese reciprocation (that is, a no-first-use pledge). This policy could clarify that counterspace and cyber attacks would be legitimate options in an outright conventional war but disproportionately dangerous in contingencies short of that. The message to China would be that the United States will not attack in these domains until the President concludes that conventional war is inevitable. The corollary is that U.S. officials would interpret Chinese attacks in these domains as a deliberate escalation. Taken together, these measures create incentives for China to forgo attacks on U.S. space and cyber assets in small-scale confrontations.

The United States could also develop conventional options for striking Chinese territory that would be tailored to managing escalation. Such options would employ a small number of U.S. assets in a short-duration strike. Importantly, U.S. officials would need to select potential military targets that meet three criteria:

- The targets would be in range of standoff weapons, so that attacking them would not require large suppression operations against Chinese air defenses; this would be essential to keep the operation small and quick.
- The targets would not be part of China's nuclear posture. This would require detailed analysis during peacetime to determine, as examples, air defense nodes, antisatellite weapons, conventional missiles, naval bases, or sensors that do not have nuclear functions.
- The targets would not be part of the regime's political leadership.

The United States could develop a spectrum of strike packages tailored to managing escalation, from an attack on a single target to larger attacks against

Launch of North Korea's Unha-3 rocket in December 2013 (Korean Central News Agency)

multiple targets that satisfy these criteria. The goal of this employment option would be to escalate by crossing a profound geographic and symbolic threshold while minimizing the chances that China would react rashly for fear of losing key strategic capabilities. U.S. officials could also follow up the operation with a cease-fire offer. Every aspect of the response would highlight the willingness to do something dangerous and the promise of reciprocal restraint. Of course, this option would entail a tradeoff with mounting an operation to dramatically degrade Chinese capabilities. Yet it may be more prudent than authorizing a larger, messier campaign for limited U.S. goals. At the least, it is an option that the President may want to consider.

This concept would probably not work after China launched a large-scale missile salvo on a U.S. base, struck an aircraft carrier, or unleashed unrelenting attacks in space and cyberspace. As a conflict progresses, the United States might need to launch large-scale conventional attacks on Chinese ISR, C2, and missiles on the mainland. The inescapable nuclear shadow means that managing escalation would remain a U.S. objective even in a high-end conventional conflict, but other military objectives would also come to the fore if U.S. and allied forces were under sustained attack.

The prospects for mutual restraint early in a conflict are most promising if the United States and China both understand the perils of inadvertent escalation. As a RAND study observes, "to reduce the risk of inadvertent escalation, the adversary . . . must *first* be enlightened, after which deterrence may or may not still be required."[38] China has thus far been suspicious of U.S. efforts to explore how a conflict between the two might spiral out of control and how they might cooperate to manage escalation, although constructive dialogues on these and other strategic issues at the unofficial level continue.[39] The escalatory danger of counterspace and cyber attacks, blurred nuclear thresholds, and nuclear signaling all merit continued discussion in these venues. China might balk, but persistent efforts to raise these issues and explain U.S. concerns would be worthwhile.

As an example, U.S. participants could explain that some in the United States would interpret China's dispersal of mobile missiles in a crisis as a provocation while others would see it as stabilizing because it reduces vulnerability and thus early-use incentives. The ultimate impact of this signal would depend on the subjective perceptions of a variety of different individuals, many of whom would have different assumptions and possibly differing information. At the least, explaining the diversity of views within the United States ensures that China's strategic community is aware of some of the complex challenges that would confront U.S. and Chinese officials during a limited conflict.

Conclusion: Institutionalizing Escalation Management

The risks of nuclear escalation in Northeast Asia will endure for years. Escalation management should be a standard metric for evaluating potential contingency and employment plans for conventional conflicts with nuclear-armed adversaries. This would help U.S. planners and policymakers scrutinize options that might be attractive for tactical military goals but carry a high strategic risk of escalation. Developing a set of criteria for assessing the escalation risks of employment plans is a good starting point:

- Would an adversary perceive a particular action as escalatory? Why?
- How might the adversary respond?
- Is this option deliberately escalatory, or is the risk of escalation a consequence of achieving a tactical objective? Are there other means for achieving these tactical objectives?
- If this option is deliberately escalatory, what is the objective and how can we mitigate the risks of the conflict getting out of control?

At the end of the day, national leaders might have little confidence in their ability to manage escalation under the nuclear shadow. Clearly, deterring potential adversaries from deciding to use force against the United States and its allies and resolving disputes diplomatically are higher priorities. But that does not obviate the need for the United States and its allies to grapple with this unpleasant topic and be as prepared as possible. **JFQ**

Notes

[1] "Assistant Secretary of Defense Madelyn Creedon, Remarks on Deterrence, Stimson Center, Washington, DC, September 17, 2013," available at <www.stimson.org/images/uploads/Creedon_Stimson_Speech.pdf>.

[2] Brad Roberts, *Extended Deterrence and Strategic Stability in Northeast Asia*, National Institute for Defense Studies (NIDS) Visiting Scholars Paper No. 1 (Tokyo: NIDS, August 9, 2013).

[3] Several recent studies of U.S.-China nuclear relations have reached this conclusion. See Elbridge Colby and Abraham Denmark, *Nuclear Weapons and U.S.-China Relations: A Way Forward* (Washington, DC: Center for Strategic and International Studies, March 2013); International Security Advisory Board, *Report on Maintaining U.S.-China Strategic Stability* (Washington, DC: Department of State, October 26, 2012); and William J. Perry and Brent Scowcroft, *Independent Task Force Report No. 62: U.S. Nuclear Weapons Policy* (New York: Council on Foreign Relations, April 2009).

[4] Office of the Secretary of Defense (OSD), *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: Department of Defense, 2013).

[5] *Joint Operational Access Concept, Version 1.0* (Washington, DC: Department of Defense, January 17, 2012); and *Air-Sea Battle: Service Collaboration to Address Anti-Access & Area Denial Challenges* (Washington, DC: Department of Defense, May 2013). See also Jan Van Tol et al., *AIRSEA Battle: A Point-of-Departure Operational Concept* (Washington, DC: Center for Strategic and Budgetary Assessments, 2010).

[6] T.X. Hammes, *Offshore Control: A Proposed Strategy for an Unlikely Conflict*, INSS Strategic Forum No. 278 (Washington, DC: NDU Press, June 2012).

[7] On North Korean capabilities, see OSD, *Annual Report to Congress: Military and Security Developments Involving the Democratic People's Republic of Korea 2012* (Washington, DC: Department of Defense, May 2, 2013); see also Jay Solomon and Julian E. Barnes, "Rocket Success Shows North Korea's Advance," *The Wall Street Journal*, December 12, 2012; Evan Ramstad, "North Korea Claims Self-Defense Against U.S.," *The Wall Street Journal*, February 13, 2013; Thom Shanker, David Sanger, and Eric Schmitt, "Pentagon Says Nuclear Missile Is in Reach for North Korea," *The New York Times*, April 11, 2013.

[8] Terence Roehrig, "North Korea's Nuclear Weapons Program: Motivations, Strategy, and Doctrine," in *Strategy in the Second Nuclear Age: Power, Ambition, and the Ultimate Weapon*, ed. Toshi Yoshihara and James R. Holmes (Washington, DC: Georgetown University Press, 2012).

[9] Keir Lieber and Daryl Press, "The Next Korean War," *Foreign Affairs* 92, no. 3 (May/June 2013); and *Coercive Nuclear Campaigns in the 21st Century: Understanding Adversary Incentives and Options for Nuclear Escalation* (Monterey, CA: U.S. Naval Postgraduate School, March 2013).

[10] Paul Bracken, *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (New York: Times Books, 2012), chapter 7.

[11] Roberts.

[12] The best discussion of the concepts and mechanics of competitions in risk taking is Thomas Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966). See also Schelling, *Strategy of Conflict* (Cambridge: Harvard University Press, 1960).

[13] *Deterrence Operations Joint Operating Concept* (Washington, DC: Department of Defense, December 2006). See also Lieber and Press, *Coercive Nuclear Campaigns in the 21st Century*, 44–46.

[14] Forrest E. Morgan et al., *Dangerous Thresholds: Managing Escalation in the 21st Century* (Arlington, VA: RAND, 2008), 7–45; see also Richard Ned Lebow, *Nuclear Crisis Management: A Dangerous Illusion* (Ithaca: Cornell University Press, 1987), 104–153.

[15] "S. Korea, U.S. to Conduct Exercise on Deterrence," Yonhap News Agency, November 4, 2011, available at <http://english.yonhapnews.co.kr/national/2011/11/04/64/0301000000AEN20111104002800315F.HTML>; and Jim Garamone, "U.S., South Korea Participate in Nuke Deterrence Exercise," American Foreign Press Service, December 5, 2012, available at <www.defense.gov/news/newsarticle.aspx?id=118716>.

[16] "Joint Communiqué: The 45th ROK-U.S. Security Consultative Meeting, October 2, 2013, Seoul," available at <www.usfk.mil/usfk/Uploads/200/Joint_Communique_45th_ROK-US_Security_Consultative_Meeting.pdf>; and Choe Sang-Hun, "U.S. Agrees to Let South Korea Extend Range of Ballistic Missiles," *New York Times*, October 7, 2012.

[17] David Sanger and Thom Shanker, "U.S. Designs a Korea Response Proportional to the Provocation," *New York Times*, April 7, 2013.

[18] Daniel Pinkston, "The New South Korean Missile Guidelines and Future Prospects for Regional Stability," *International Crisis Group Strong and Prosperous Blog*, October 25, 2012; Yuka Hayashi and Julian E. Barnes, "U.S., Seoul Plan Response in Case of North Korean Attack," *Wall Street Journal*, March 26, 2013; and Richard Weitz, "North Korean Threats Deepen Southern Nuclear Insecurities," *Diplomat*, July 4, 2013.

[19] Abraham M. Denmark, *Proactive Deterrence: The Challenge of Escalation Control on the Korean Peninsula*, On Korea: Academic Paper Series (Washington, DC: Korea Economic Institute of America, December 2011).

[20] Ken E. Gause, *North Korean Calculus in the Maritime Environment: Covert Versus Overt Provocations* (Alexandria, VA: Center for Naval Analyses, July 2013). Gause argues that retaliation for proportionate South Korean responses to overt provocations is unlikely because the initial attacks were probably motivated by a desire to reinforce North Korean statements and redlines, whereas North Korean covert provocations are motivated by internal dynamics and regime powerbrokers' concerns about their own weaknesses relative to others in the regime, and therefore retaliation is more likely.

[21] Roberts; James L. Schoff, *Realigning Priorities: The U.S.-Japan Alliance and the Future of Extended Deterrence* (Cambridge, MA: Institute for Foreign Policy Analysis, 2009). Both analysts are referring to the U.S.-Japan alliance, but the insight is relevant to the U.S.-ROK alliance as well.

[22] Chico Harlan, "N. Korea warns of 'moment of explosion,' bans South's workers from border factory," *Washington Post*, April 3, 2013; Choe Sang-hun, "North Korea Moves Missile to Coast, but Limited Threat Seen," *New York Times*, April 4, 2013.

[23] In a statement released several days before she took office and several days after North Korea's third nuclear test, President Park Geun-hye pledged that "Missile capability will be expanded to develop a 'Kill Chain' system to preemptively strike North Korean missile launchers and nuclear facilities." See Sangwon Yoon, "Park Lists Top Priorities as South Korean Jobs, North Deterrence," *Bloomberg.com*, February 21, 2013; "Defense Ministry: NK Nuclear," Yonhap News Agency, March 31, 2013; Julian Barnes, In-Soo Nam, and Kwanwoo Jun, "U.S. Moves Missile Destroyer Near North Korea," *Wall Street Journal*, April 1, 2013; "South Korea Selects the Taurus KEPD 350 Cruise Missile," *Defense Update*, April 5, 2013; and Kim Eun-jung, "State Arms Procurer Requests 11 [Trillion] Won Budget for Next Year," Yonhap News Agency, June 18, 2013.

[24] Lieber and Press, *Coercive Nuclear Campaigns in the 21st Century*, 46.

[25] Avery Goldstein, "First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations," *International Security* 37, no. 4 (Spring 2013), 49–89; and Vincent Manzo, "The Threat that Leaves Something to Chance in U.S.-China Relations," *Nuclear Scholars Initiative: A Collection of Papers from the 2011 Nuclear Scholars Initiative* (Washington, DC: Center for Strategic and International Studies, 2011).

[26] Van Tol et al.

[27] Goldstein argues that China's perceptions of asymmetric stakes would be a likely driver of miscalculation and escalation in U.S.-China crises.

[28] Elbridge Colby, "Don't Sweat AirSea Battle," *The National Interest*, July 31, 2013.

[29] Scott Sagan, "Deterring Rogue Regimes: Rethinking Deterrence Theory and Practice," Center for International Security and Cooperation, July 8, 2013, 11–12.

[30] For a thorough analysis of U.S. and Chinese strategic thinking on offensive cyber and counterspace operations, see David C. Gompert and Phillip C. Saunders, *Paradox of Power: Sino-American Strategic Restraint in an Era of Vulnerability* (Washington, DC: NDU Press, 2011), chapters 1, 2.

[31] Hammes; Goldstein; and David C. Gompert and Terrence Kelly, "Escalation Cause: How the Pentagon's New Strategy Could Trigger War with China," *Foreign Policy*, August 2, 2013.

[32] Vincent Manzo, *Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyber Fit?* INSS Strategic Forum No. 272 (Washington, DC: NDU Press, December 2011).

[33] For a discussion of the potential for accidents or incidents between U.S., Japanese, and Chinese air and naval forces in the region, see Shawn Brimley, Ben Fitzgerald, and Ely Ratner, "The Drone War Comes to Asia," *Foreign Policy,* September 17, 2013.

[34] Thomas Christensen, "The Meaning of Nuclear Evolution: China's Strategic Modernization and U.S.-China Security Relations," *Journal of Strategic Studies* 35, no. 4 (August 2012); and Christopher P. Twomey, "Asia's Complex Strategic Environment: Nuclear Multipolarity and Other Dangers," *Asia Policy*, no. 11 (January 2011). For discussions of Chinese concerns about U.S. conventional strikes on nuclear forces, see Lora Saalman, *China and the U.S. Nuclear Posture Review* (Washington, DC: Carnegie Endowment for International Peace, February 2011), 22–26; and Thomas Fingar, "Worrying About Washington: China's Views on the U.S. Nuclear Posture," *Non-Proliferation Review* 18, no. 1 (March 2011). See Van Tol et al., 56–69, for a discussion of how the United States might suppress China's conventional missile force in the ASB concept.

[35] For a discussion of China's nuclear employment plans, see M. Taylor Fravel and Evan S. Medeiros, "China's Search for Assured Retaliation: The Evolution of Chinese Nuclear Strategy and Force Structure," *International Security* 35, no. 2 (Fall 2010).

[36] Michael Chase, "China's Transition to a More Credible Nuclear Deterrent: Implications and Challenges for the United States," *Asia Policy*, no. 16 (July 2013).

[37] The 2010 *Nuclear Posture Review Report* identified visibly forward-deploying nuclear-capable bombers as a valuable capability for signaling U.S. resolve in crises, and in March 2013, the United States publicized that nuclear-capable B-2 bombers conducted test runs over South Korea during a period of heightened tension with North Korea. See *Nuclear Posture Review (NPR) Report* (Washington, DC: Department of Defense, April 2010), 24; and Thom Shanker and Choe Sang-Hun, "U.S. Runs Practice Sortie in South Korea," *The New York Times*, March 28, 2013.

[38] Morgan et al., 24–25.

[39] Ralph Cossa, Brad Glosserman, and David Santoro, "Progress Continues, but Disagreements Remain: The Seventh U.S.-China Strategic Dialogue on Strategic Nuclear Dynamics & The Inaugural China-U.S. Dialogue on Space Security," *Issues and Insights* 13, no. 6 (January 2013). On the role and value of unofficial and official strategic dialogues with China, see Colby and Denmark, *Nuclear Weapons and U.S.-China Relations.*

Sailors work on flight deck as aircraft carrier USS *Nimitz*, conducting maritime security operations and theater security cooperation efforts, transits Straits of Malacca (U.S. Navy/Derek A. Harkins)

Fighting More Fires with Less Water

Phase Zero and Modified Operational Design

By Tyrone L. Groh and Richard J. Bailey, Jr.

In the last decade, our foreign policy has transitioned from dealing with the post–Cold War peace dividend to demanding commitments in Iraq and Afghanistan. As those wars wind down, we will need to accelerate efforts to pivot to new global realities. We know that these new realities require us to innovate, to compete, and to lead in new ways. Rather than pull back from the world, we need to press forward and renew our leadership.

—Secretary of State Hillary Clinton, 2011

Imagine that you are the fire chief for a mid-sized community. The city council informs you that it is reducing your budget this year by 30 percent. It is redirecting these funds for community outreach and fire-prevention education programs. Ironically, the council has also instructed you to organize and conduct these programs. In every previous year, you have used the entire budget to train and equip your firefighters and to respond to fire emergencies in the city. You know that outreach is important and may indeed help to lower the incidence of fires in the city—assuming, of course, that your city is not rife with arsonists. However, will you now have sufficient resources to accomplish your primary mission? Put another way, is *putting out* fires or *preventing* them a better use of your resources?

This fire-fighting/prevention metaphor helps to inform a current and pressing military conundrum. With limited and shrinking budgets, how should the United States balance efforts to *prepare for war* versus efforts to *prevent war*? Does the adage "an ounce of prevention

Lieutenant Colonel Tyrone L. Groh, USAF (Ret.), Ph.D., is an Associate Professor of Political Science in the College of Global Security and Intelligence Studies at Embry-Riddle Aeronautical University in Prescott, Arizona. Colonel Richard J. Bailey, Jr., USAF, is a Professor of Strategy and Security Studies and the Dean of Students at the School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama.

PLAN rear admiral drinks sample of purified water at disaster site in Biang, Brunei Darussalam, as engineers with China, Singapore, and the United States demonstrate water purification capabilities (U.S. Marines/Kasey Peacock)

is worth a pound of cure" hold in this context? We argue it does. America has to find a way to optimize its resources without losing sight of the fact that the primary responsibility of its Armed Forces is to fight and win the Nation's wars. Theater commands, such as U.S. Pacific Command, are already working on using engagements to create favorable conditions if any actor attempts to challenge its interests in the region.

We argue that, first, U.S. political and military leaders must conceptualize Phase Zero operations more broadly than simply shaping the preconflict battle zone; rather, they should think of them as a complex, long-term, grand preventative strategy. Second, military planners should seek indicators for potential leverage points that help senior military leaders make educated, efficient, and effective decisions regarding the use of U.S. assets. These efforts will not prevent every conflict, but they should reduce the number of conflicts and preserve resources for when they are needed most. Such an activity requires a coherent vision that maps out how to move from the present situation toward a desired future environment.

Let us consider a real-world example. In November 2011, Secretary of State Hillary Clinton signaled two noteworthy shifts in U.S. policy. The first was geographic: namely a transition from attention on the Middle East to a stronger focus on the Asia-Pacific region. The second sought to change fundamentally the type of international engagement to which the United States, particularly its Armed Forces, had grown accustomed, a change that reflected a more preventative rather than responsive mentality.[1] The decade-long combat operations in Iraq and Afghanistan were showing their first signs of winding down. The American public, reminded of the significant costs of two wars in lives and dollars and struggling with domestic challenges, was growing weary of military and foreign entanglements. Thus, the "Pivot to Asia" required a nuanced approach to promote and protect national interests abroad while at the same time obviating increasing public concern for America's continual involvement in world affairs.

One solution seeks to make military engagement less lethal; U.S. forces should rebalance efforts to focus on dialogue, key leader interaction, building partner capacities and capabilities, encouraging bilateral and multilateral cooperation, and cultivating enduring international norms that support American interests. The U.S. military, however, needs to be careful about when and where it chooses to engage; gains in one place often mean lost ground in another. For example, engagements with

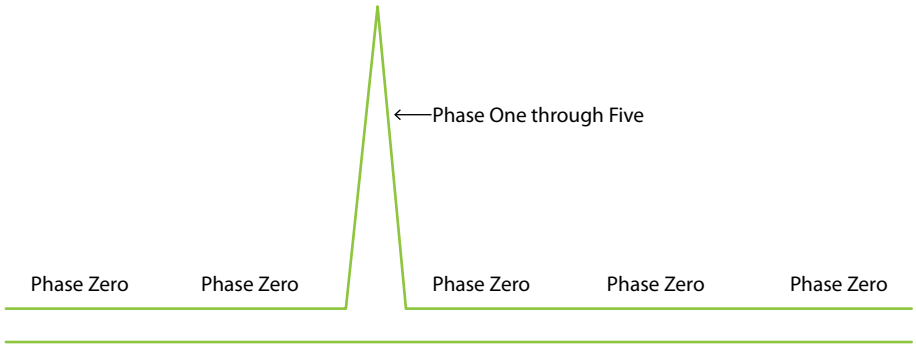
India may deepen Indo-U.S. relations, but they hamper U.S. relations with China and Pakistan. It is no surprise that the key to these types of efforts is to make the gains outweigh the losses in the long term. Properly considered, Phase Zero operations should do just that. We must stop considering Phase Zero as a means to prepare for major combat operations (MCOs). Phase Zero operations must become tied to the long-term vision within which short periods of Phases I through V operations occur (see figure 1). Our hope is that such a vision minimizes the likelihood that decisions will be made based on short-term gains with no consideration for potential long-term losses.

Figure 1 depicts a significant oversimplification, but it illustrates the point that Phase Zero operations should be ongoing, with the intent of preventing the frequency and severity of MCOs when they do occur.

Despite even the most successful Phase Zero efforts, MCOs will still be necessary from time to time, so the Armed Forces must remain prepared for those eventualities. If done well, however, Phase Zero operations should support MCOs either directly or indirectly. The problem we are trying to fix is the use of Phase Zero operations to support and prepare for a potential MCO; this kind of thinking potentially undermines the long-term pursuit of an advantageous geopolitical environment in exchange for more short-term objectives.[2]

Consider a Phase Zero engagement with India. U.S. policymakers consider the Straits of Malacca a potential area of conflict. Cultivating relationships in the region not only allows for a combined effort should conflict become necessary, but also focuses limited resources toward prevention while reserving others for unforeseen circumstances. The change we propose requires a mental shift from a concept of Phase Zero operations that support universal American dominance in *every* region and theater to one of focusing on efforts that minimize conflict—or, just as importantly, the American role in conflicts—and enable America to retain the resources necessary to ensure dominance in the most vital areas. This means accepting less control globally in exchange for less conflict or less expense in dealing with conflicts in less critical areas should they arise. In other words, Phase Zero operations cultivate relationships in places where we can count on partners for support in areas important, but not necessarily vital, to U.S. national security interests. As a result, Phase Zero operations should help America make more resources available when it chooses the specific places in which it will defend its most important interests. Additionally, Phase Zero operations can potentially decrease the resources required to defend interests in vital locations based on the relationships developed in peripheral areas.

Figure 1. Hypothetical Chronology of Phases Zero through Five



The second part of our argument calls for a modification to operational design when applied to Phase Zero operations. Operational design has the potential to enhance military decisionmaking. As General James Mattis, USMC, declared in 2009, "The complex nature of current and projected challenges requires that commanders routinely integrate careful thinking, creativity, and foresight. Commanders must address each situation on its own terms and in its unique political and strategic context rather than attempting to fit the situation to a preferred template."[3] While we support the use of operational design as the preferred process to help military planners, operational design for Phase Zero should be modified from the template we use for MCO. Using MCO operational design processes can confuse Phase Zero planning because there is a significant difference in focus between planning to implement the use of lethal force and implementing efforts that will avoid or alleviate the *need* to use lethal force.

In the next section, we explore Phase Zero operations and illustrate how their etymology and process structure are still rooted in an MCO construct and therefore may hamper effective Phase Zero planning. Finally, we offer a modified Phase Zero operational design model for consideration based on the concepts of *inflection points* and *emerging opportunities*, a model that has the potential to optimize the conceptualization and planning of this recently articulated military enterprise.

The Long Game

In 2001, the United States undertook a prodigious military effort to rid the world of dangerous terrorist networks that could operate on a global scale. The enormity of that effort precluded the United States from doing it alone. The 2010 National Security Strategy (NSS) described the need for engagement for the purposes of "combating violent extremism, stopping the proliferation of nuclear weapons, and addressing the challenges of climate change, armed conflict, and pandemic disease."[4] *Phase Zero*, as defined by General Charles Wald, USAF, was intended to preserve U.S. resources by accomplishing those tasks through engagement rather than through lethal means. The current view articulated in Joint Publication 5–0, *Joint Operation Planning*, however, undermines this broader perspective of Phase Zero and bounds the idea to shaping operations that support MCO.

Sailors stand watch on bow of *Arleigh Burke*–class guided-missile destroyer USS *McCampbell* as ship enters Straits of Malacca in support of security and stability in Indo-Asia-Pacific region (U.S. Navy/Paul Kelly)

Phase Zero operations should focus on building cooperative relationships with states around the world in a way that will enhance continued national security and prosperity. In many cases, military channels offer opportunities to gain access to and build trust between both new and existing partners. Military education, training, and exchanges provide easy opportunities for engagement without the high levels of political scrutiny that often accompany similar opportunities at the diplomatic level. As an added benefit, such activity builds epistemic communities among those at lower levels based on their shared experiences.[5] Such advantages can lead to greater influence at higher levels when difficult diplomatic incidents occur (for example, the arrest of an Indian diplomat in December 2013).[6] Phase Zero requires a high level of integration between geographic combatant commands and the Country Teams led by each U.S. Ambassador. For many other agencies in the U.S. Government, nonlethal foreign engagement is the primary focus. For example, the United States Agency for International Development states, "The most important thing we can do is prevent conflict in the first place. This is smarter, safer, and less costly than sending in soldiers."[7] For the Department of Defense, however, the majority of effort focuses on organizing, training, and equipping forces to fight and win the country's wars. Making matters worse, military planning and training for Phase I–V operations compete for resources with Phase Zero requirements. Money spent building relationships and increasing the capacity of others takes away from money available to make U.S. forces more capable. Additionally, the rotation of commanders in the different geographic combatant commands places a premium on short-term investments—those that support emphasis on Phases I–V.

Phase Zero, properly conceived and conducted, requires a long-term investment strategy that transcends successive commanders. The information available and progress achieved during Phase Zero are relatively opaque and ambiguous. Therefore, senior leaders are not going to be able to measure success by any observable—or for that matter, *reportable*—account over short periods of time. This makes motivating the people doing the Phase Zero mission challenging and increases the difficulty of measuring performance at the highest levels of command. Senior leaders have to adapt from seeking progress-oriented, task-driven constructs, such as operational planning for major combat operations, to open time horizons and outcomes that are fraught with ambiguity. Phase Zero must include considerations and preparations for incongruities between executing planned activities and responding to a potential or actual crisis that would hinder progress toward the desired condition.

Phase Zero should be about preventing conflicts, but it should also be a commitment to cultivating partners and

building relationships that enable the United States to achieve and maintain security and prosperity. In a world of growing scarcity, the Nation will have to compromise more to achieve both. The 2014 Quadrennial Defense Review alludes to this quest:

Our sustained attention and engagement will be important in shaping emerging global trends, both positive and negative. Unprecedented levels of global connectedness provide common incentives for international cooperation and shared norms of behavior, and the growing capacity of some regional partners provides an opportunity for countries to play greater and even leading roles in advancing mutual security interests in their respective regions.[8]

Our concept of Phase Zero operations can enhance American security, but it requires a shift in perspective. The unipolar moment is waning, and the United States must come to grips with a complicated post–Cold War global system that offers rewards to its members more equitably than it did in the last decade of the 20th century. The United States no longer has the means required to influence the global system in a way that makes it the clearly dominant power. This state of affairs is foreign to planning for major combat operations—an endeavor in which there is usually a winner and a loser.

Facilitating Quality Decisionmaking

To stay ahead of the frenetic pace of today's military commanders, effective staff members use operational design to make sense of the complex operational environment, distill military efforts into categorized segments, and determine nodes that require commanders' decisions. Ideally, staffs will attempt to predict these decision points and inform the commander of the factors he or she should consider when making those critical decisions. Turnover on military staffs and a lack of continuity among planners, however, have prompted many in the U.S. military to turn operational design into a mechanistic process that essentially requires those involved to "fill in the blanks." It has produced a culture that unknowingly believes that the process itself, rather than the critical thinking for which operational design was created, is the end product.

Figure 2. Acquisitions Lag-Time and Workarounds

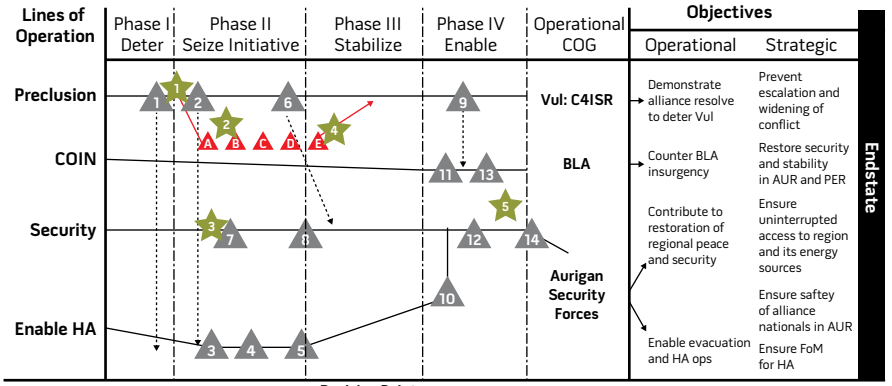


Figure 2 illustrates an example of an operational design product depicting lines of operation.[9] The yellow stars indicate decision points where there is an expectation of a commander's decision; this decision typically either takes advantage of exploited opportunities or rebalances an effort based on changes in the operational environment. In addition to expected shifts or advances in the operational effort, staffs should analyze the operational environment to identify potential *emerging* situations, so that if they do arise, they may provide advantageous *opportunities.* Ultimately, operational design is a mechanism that, when properly applied, helps staffs to think about the contextual and temporal complexities of the environment that they are operating in. This awareness enables them to assist their commanders in conceptualizing the environment and overall operation and to make educated decisions about applying limited resources in support of a coherent strategic vision.

This section does not review the details of operational design. Jeffrey Reilly and others have done a fine job of explaining that process, and we wholeheartedly support its more widespread use. Reilly's model provides a useful and effective method of planning for Phases I through V. But upon examination, it is clear that operational design (as it is currently used) is based on a construct of major combat operations. Three aspects of current operational design highlight this foundation: military end state, center of gravity, and decisive points.

In major combat operations, joint doctrine defines the *military endstate* as the "set of required conditions that defines achievement of all military objectives."[10] The guidance is unclear as to the best way to define that endstate. But without question, the term itself connotes (and actually denotes) a *cessation* of military activities: "It normally represents a point in time and/or circumstances beyond which the President does not require the military instrument of national power as the primary means to achieve remaining national objectives."[11] As the analysis in the previous section indicated, no such end point exists in Phase Zero. Rather, the centerpiece of Phase Zero operations is the cultivation of *enduring*, synergistic relationships.

Cavalry scout and Indian army counterpart provide security for fellow soldiers during patrol through forests of Himalayas during exercise Yudh Abhyas (DOD/Mylinda DuRousseau)

The term *center of gravity* finds its origin in Carl von Clausewitz's seminal 1832 treatise *On War:* "[One] must keep the dominant characteristics of both belligerents in mind. Out of these characteristics a certain center of gravity develops, the hub of all power and movement, on which everything depends. That is the point against which all our energies should be directed."[12] In MCOs, a commander looks for ways to direct friendly forces in effective ways. Understandably, this is done in an effort to minimize losses and prevent prolonged confrontation. Therefore, the most frequently used rule of thumb is that if you can discover the enemy's center of gravity and direct your efforts there, you will have the greatest effect. In addition, if you conduct a center of gravity analysis on your own forces, you can better consider defensive posturing.

As Antulio Echevarria explains, however, the U.S. military's definition of center of gravity has both evolved and diverged over time. The concept should not, in fact, be "applied to every kind of war or operation; if it is, the term may become overused and meaningless or be conflated with political-military objectives."[13] Centers of gravity were the centerpiece of John Warden's Five-Ring Model, used most famously in the planning of the air campaign in Operation *Desert Storm* and also in Joe Strange and Richard Iron's Critical Vulnerability construct, which drills down from centers of gravity to guide the development of actual target sets.[14] In Phase Zero operations, however, there is no clearly defined enemy against which commanders can direct their focus. How will a commander know where to place limited resources to have the optimal outcome? Ultimately, a center of gravity analysis for Phase Zero operational designs (at least as it is used today) is problematic.

Joint doctrine posits that a thorough center of gravity analysis will shed light on possible *decisive points*:

A decisive point is a geographic place, specific key event, critical factor, or function that, when acted upon, allows a commander to gain a marked advantage over an adversary or contributes materially to achieving success. . . . Although decisive points are not COGs [centers of gravity]*, they are the keys to attacking protected COGs or defending them. Decisive points can be thought of as a way to relate what is "critical" to what is "vulnerable." Consequently, commanders and their staffs must analyze the operational environment and determine which systems' nodes or links or key events offer the best opportunity to affect the enemy's COGs or to gain or maintain the initiative.*[15]

Consider, from the perspective of major combat operations, the logical flow of endstate, center of gravity, and decisive points. What follows is perhaps an oversimplification of the process. But to put it concisely, the military strategist works backward from an endstate to conduct a center of gravity analysis on the enemy, determine critical vulnerabilities that illuminate decisive points, and then (with military planners) group similar decisive points into clearly defined lines of operation or effort. As Keith Dickson writes, "By determining the critical vulnerabilities of the enemy center(s) of gravity, planners have a means to determine decisive points related to attacking those critical vulnerabilities."[16] In MCOs, this seems fairly straightforward. Decisive points are aptly named because they designate where military efforts can concentrate forces to enable mission success. But like *endstate* and *centers of gravity*, the term *decisive point* signifies a finite effort directed at an enemy force within a specified timeframe. Phase Zero efforts are radically different, often open-ended efforts without a defined enemy and without a specified culmination point.

We are not suggesting turning military forces into full-time diplomats, but we firmly acknowledge that the military Services have a large role to play in Phase Zero. To increase effectiveness, planning efforts require a significant shift from current conceptions to allow a more productive relationship between military and other government agencies—especially Country Teams working under their Ambassadors. This effort is put forth with the recognition that the military's greatest asset is its ability, when called upon, to wage war to meet national objectives and to organize, train, and equip its forces so that its readiness serves as a constant deterrent to would-be aggressors.

During Phase Zero operations, the military still exercises its traditional influence but in a different way and with significantly different political objectives. Thus, the military Services must be much more creative in how they think about and plan these efforts. *Creative thinking* might be defined as "consciously generating new and useful ideas, and re-evaluating or combining old ideas, to develop new and useful perspectives in order to satisfy a need."[17] But optimizing creative thinking requires a dismantling of framed approaches. As Susan Carter eloquently

puts it, "Word choice matters. Sometimes a word skews the whole thread of discussion off track by smuggling in with its connotations a set of ideas that are counter to your own epistemological position."[18] Semantics are important because words have a tendency to feed biases or solidify frames that can stifle creative thinking.

Inflection Points and Emerging Opportunities

Words or phrases such as *adversary* or *decisive points* that military planners use in operational design alter the perspective of the planning process. We argue that a shift in focus to two particular terms will significantly change a commander and staff's view of Phase Zero operations. The first term we suggest is *inflection point*, which we define as the moment in time when the normal progression of a particular phenomenon significantly changes. For example, India has a reasonably predictable water supply. India's birth rates and infant mortality rates remain relatively predictable over time as well. At some point in the future, however, India's population will exceed its water resources. That predictable fact enables a planning staff to identify a logical inflection point.

An inflection point is particularly important in the development of strategy because it identifies a period of such intense change that the actor experiencing the change has not had time to adjust to it. At best, the actor will still be in the early stages of the adaptation phase. It is during this phase that the actor most needs to find some means of adapting to the new situation. An outside actor may be of significant assistance and a helpful influence during this particular period. For example, if you lived in an area with high forest fire potential and learned early in the morning that a forest fire was going to burn your house down at midnight, you would likely resist the efforts of an outsider coming in to assist you in your evacuation. You would have sufficient time to take the necessary safety precautions to gather important documents and valuables and be long gone when the fire took your house. But if you imagine a scenario in which you were in a low fire potential area and you only had 30 minutes of notice, and the same outsider arrived to assist you, would you be more likely to accept help? Perhaps. What if the outsider showed up with a moving van and 20 people to help you get whatever you wanted to take with you? Probably. Finally, what if the outsider and his crew had significant experience with such situations and were willing to offer advice about how to handle the evacuation? Under those conditions, an outsider would be influential, even more so if you had practiced evacuations with the outsider on several previous occasions.

In this example, the inflection point was the shift from the potential for a forest fire to the near certainty that it would occur. Planning staffs should be looking for potential inflection points and align engagements that will position the United States to respond and influence the situation. Inflection points become particularly important because they focus resources in areas with the highest level of influence during a period of shrinking budgets and severely constrained resources. Resources have to be allocated more effectively in the future to enable America to maintain the same level of influence as it had in the past. Inflection points are also important because they represent likely swings in the status quo. For Phase Zero operations, the intent is to prevent these large swings from creating conditions inimical to American interests. Identifying and preparing for inflection points put the United States in a position to stamp out a spark before it becomes a forest fire.

The second term we want to introduce is *emerging opportunity*. To illustrate the concept, let us refer back to the firefighter analogy and the hypothetical Indian example. Suppose that as the fire chief, your community is faced with an unforeseen drought, which has caused water prices to skyrocket. Coupled with this (and solely for the purpose of this scenario), you worry that there may not be enough fire hydrants in the area to meet your expected response needs. The water shortage and related cost hike are significant enough that many residents have been priced out of filling their backyard swimming pools. But with your access to cheaper water, you initiate a program whereby the fire department fills pools for free on request. The only stipulation is that the residents must agree to give you access to the pool water if needed to assist in fire response. Taken a step further, you could even encourage a program whereby the fire department actually subsidizes construction of more backyard pools in the area. In both of these cases, an unforeseen circumstance—the drought—actually creates an opportunity for increased engagement that may further your long-term interests. Contributing the pool water not only strengthens your connection to the local populace (through the tacit agreement), but also provides a distributed, risk-mitigating resource to assist with your primary firefighting responsibilities should the need arise.

Let us now build on the concept by returning to our hypothetical Phase Zero engagement effort with India. The goals of the effort are to make India a regional leader in international security efforts, while at the same time fostering a bilateral relationship advancing U.S. interests in the region. With little warning, a massive typhoon hits the southern portion of the Andaman Sea, threatening catastrophic destruction to the Andaman and Nicobar Islands, the western coast of southern Thailand, and the northern coast of Indonesia. As the United States has done in similar cases, it redirects military forces to aid (and perhaps even lead) humanitarian relief efforts. Engagement such as this is nothing new. But from a Phase Zero perspective, is it possible that the humanitarian relief might actually create new avenues for interaction with India? The semantics of this point are important. No natural disaster should ever be seen as an *opportunity* per se, but in the realm of military engagement and relationship cultivation, military leaders and planning staffs should consider how partnerships in unforeseen circumstances can actually further Phase Zero initiatives.

Imagine a scenario in which India and the United States work together to direct a humanitarian airlift to Phuket in western Thailand, which suffered the most devastating damage from the typhoon. Where is the opportunity here?

Put simply, the partnership with India in directing airlift aid offers a chance not only to work together toward limited short-term goals (including, obviously, assistance to the victims of the crisis), but also to demonstrate U.S. response techniques in the hope that India takes a larger role in similar regional crises in the future. Ultimately, India might be able to handle such tasks independently (in a way resembling American-style responses). A larger Indian presence in disaster relief in the region might provide area stability consistent with U.S. foreign policy goals and help India to reach its own goals as a rising regional power. It also frees American military resources to respond to crises (or worse, conflict) in areas where the United States does not have similar relationships. This is the cornerstone of Phase Zero engagement.

For planners, unforeseen events are just that: unforeseen. But it does not mean that Phase Zero planning should ignore their possibility (indeed, even their likelihood, given the long-term nature of Phase Zero operations). Any Phase Zero planning should contemplate emerging opportunities that may offer immediate engagement and foster stronger relationships; it must also be flexible enough to re-prioritize efforts accordingly. In addition, similar to the branch and sequel concept of MCO operational design, planners should consider such diversions in terms of their impact on major lines of operation or effort in a Phase Zero construct.

Conclusion

A common dictum among military professionals is *si vis pacem, para bellum*—if you want peace, prepare for war. Strategists and military planners continue to act in a way that places a high emphasis on following this dictum. The United States needs to continue preparing its forces against future threats; we make no argument against that. We argue, however, that preparing for war is an expensive endeavor and that adjustments must be made as resources become increasingly scarce and as other states begin to challenge American dominance in areas that contribute to U.S. and global prosperity. Strategy and planning must become more pragmatic, and spending must focus more on the efficiencies of investing in prevention, rather than paying the enormous costs associated with cures.

Changing the way we think about Phase Zero is a beginning to such an effort. Phase Zero as a means to prevent war is fundamentally different from the current thinking that sees it as a means to prepare for war. If Phase Zero thinking subsumes Phases I through V, it can promote a coherent vision for how to conduct relations and engagements with other states or actors that can contribute to the stability of the global commons and international norms.

Strategists and military planners must concentrate on preventing wars before they start or, at the least, forming strong networks of partners that make defeating troublemakers or would-be adversaries much easier. To that end, the United States must identify key inflection points and emerging opportunities that propel Phase Zero operations in a direction that increases the influence of either the United States or its partners. In some cases, our long-term interest may require putting a partner's short-term interest first—a notion that America has not had to face since the end of World War II. The United States must become more adept at shaping and nudging actors and conditions rather than relying on its own resources to fix problems. Put another way, it is drought season, and water is getting increasingly scarce. America has to change its thinking to be more effective at *preventing* fires and at conserving its precious resources so that when they *do* ignite, its Armed Forces are ready. JFQ

Notes

[1] Hillary Clinton, "America's Pacific Century," *Foreign Policy* 189 (November 2011), available at <www.foreignpolicy.com/articles/2011/10/11/americas_pacific_century>.

[2] While Phase Zero in our conceptual framework is a global enterprise, combatant commanders will have to make decisions on the prioritization of limited engagement resources.

[3] General James Mattis, USMC, "Memorandum for U.S. Joint Forces Command: Vision for a Joint Approach to Operational Design," October 6, 2009, in U.S. Joint Forces Command, Joint Doctrine Series Pamphlet 10, *Design in Military Operations—A Primer for Joint Warfighters*, September 20, 2010, 2.

[4] *National Security Strategy* (Washington, DC: The White House, May 2010), 3.

[5] For more on epistemic communities, see Peter Haas, "Introduction: Epistemic Communities and International Policy Coordination," in *International Organization* 46, no. 1 (Winter 1992).

[6] On March 31, 2014, the U.S. Ambassador to India, Nancy Powell, resigned after a sharp decline in India-U.S. relations. Many believe that one of the events precipitating this decline was the arrest of Deputy Consul-General Devyani Khobragade in New York City in December 2013 on charges of visa fraud. For more details, see <http://thediplomat.com/2014/04/us-ambassador-to-india-resigns/>.

[7] For more on the United States Agency for International Development's mission goals, see <http://www.usaid.gov/what-we-do>.

[8] Department of Defense, *Quadrennial Defense Review 2014* (Washington, DC: U.S. Government Printing Office, 2014), iii.

[9] Jeffrey M. Reilly, *Operational Design: Distilling Clarity from Complexity for Decisive Action* (Montgomery AL: Air University Press, 2012), 78.

[10] Joint Publication 5-0, *Joint Operation Planning* (Washington, DC: The Joint Staff, August 11, 2011), xxi.

[11] *The Joint Forces Operations and Doctrine Smartbook: Guide to Joint, Multinational and Interagency Operations*, 2nd Revised Edition (Lakeland, FL: The Lightning Press, 2009), 3–24.

[12] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 595–596.

[13] Antulio J. Echevarria II, "Clausewitz's Center of Gravity: It's Not What We Thought," *Naval War College Review* LVI, no. 1 (Winter 2003), 118.

[14] John A. Warden III, "The Enemy as a System," *Airpower Journal* 9 (Spring 1995), 40–55; Joe Strange and Richard Iron, "Understanding Centers of Gravity and Critical Vulnerabilities," U.S. Department of the Air Force.

[15] *The Joint Staff Officer's Guide*, Joint Forces Staff College, National Defense University, August 13, 2010, 4–51.

[16] Keith D. Dickson, "Operational Design: A Methodology for Planners," *Campaigning* (Spring 2007), 26.

[17] School of Advanced Military Studies, *Art of Design: Student Text Version 2.0* (Fort Leavenworth, KS: U.S. Army Combined Arms Center, 2010), 63.

[18] Susan Carter, "Finishing the Thesis: Personal Relationship with Writing," *Wordpress.com*, November 9, 2012. Full entry can be found at <http://doctoralwriting.wordpress.com/2012/11/>.

Airmen balance weight of U-2 Dragon Lady, which delivers critical imagery and signals intelligence to decisionmakers throughout all phases of conflict (U.S. Air Force/Marie Brown)

Distributed Common Ground System—Future

Moving into the 22nd Century Today

By Eugene Haase

While supporting a free medical clinic in western Afghanistan, U.S. and coalition forces question local villagers about an increase in recent enemy activity. They learn of unusual vehicle movements and a larger number of fighters in the village over the past several weeks. After returning to base, this information is passed to the unit intelligence officer who annotates it in an initial report that is made available through a shared intelligence database. Several hours later, a known enemy signal is intercepted not far from the village and is passed by way of secure joint chat rooms and product reports. At nearly the same time, advanced imaging data from a Navy Triton unmanned aerial vehicle (UAV) shows unusual disturbances in the same area. Shortly thereafter, an Army unit begins a patrol in the vicinity with a Shadow UAV performing overwatch. As the patrol reaches the area where the disturbances were noted, they are ambushed and take significant losses.

Major General Eugene Haase, USAF, is Vice Commander of Air Force Special Operations Command. He was formally the Director of Intelligence, Surveillance, and Reconnaissance, Headquarters Department of the Air Force.

Joint terminal attack controller sights target with AN/PED-1 Lightweight Laser Designator Rangefinder to mark simulated hostile threats for air assets (U.S. Marine Corps/Devon Tindle)

While notional, this scenario highlights a problem: Department of Defense (DOD) inability to conduct tailored data-sharing between processing and exploitation facilities. Unfortunately, the information necessary to warn the patrol of enemy activity is most likely available in various systems and databases, along with an overwhelming amount of valuable intelligence not necessarily pertinent to this specific mission. Today, DOD has limited automated tools available to pick this relevant information out of the trillions of bits of data routinely collected. There is only a rudimentary combined information-sharing architecture to ensure that the right person gets the right information at the right time. A key missing link is that the intelligence professionals processing and exploiting data streams from different sensors do not operate in a single collaborative environment where all applicable information is cross-displayed, allowing analysts awareness and mission synchronization between collection sensors.

Without this shared picture, the mission operation commander of the processing, exploitation, and dissemination (PED) crew does not have a real-time or complete view of the battlespace, which would have allowed them to detect the advancing ambush and warn the patrol. Although this scenario highlights a permissive counterterrorist environment, the lack of PED interoperability and a shared common intelligence, surveillance, and reconnaissance (ISR) picture is a factor regardless of the operational setting.

Expanding PED Capability

Operational usefulness of a shared information environment, combined with declining budgets, new technologies, and the future strategic landscape, is driving the need for more collaborative PED. The merging of joint, interagency, and coalition partner PED capabilities leads us down the path of better and more efficient warfighter support.

The concept of a global federated PED enterprise builds upon existing and emerging capabilities where the PED task can be quickly assigned to the most qualified entity to process and analyze the data anywhere, regardless of the sensor, and then pass it on to support any shooter and/or decisionmaker at the right place and time. The organization or platform providing the intelligence should be indistinguishable to the customer.

The global federated PED concept would allow each joint, interagency, or coalition member to continue to build on his own core competencies without recreating or duplicating the core competencies of others. This future PED enterprise is achievable, but requires buy-in from all stakeholders and more attention to community standards and policies. The Distributed Common Ground System–Future (DCGS-Future) requires a proactive effort to move to this structure now, during a time of declining budgets.

The Value of ISR

Over the past 13 years, the conflicts in Iraq and Afghanistan have unquestion-

ably demonstrated the value of ISR—particularly airborne ISR. Ongoing investment and modernization by the Services, Intelligence Community (IC),[1] and our coalition partners—as well as the increasing number and type of ISR collection platforms to meet future situations of national interest—reflect this.

Airborne ISR collection has moved well beyond the historic capabilities of still imagery and basic radio intercept/direction finding. State of the art development has led to multi- and hyperspectral sensing across a broad range of the electromagnetic spectrum, wide-area motion imagery, high-definition full-motion video, light detection and ranging, advanced radar-sensing, and advanced motion detection and tracking. Optimal use of ISR now requires much more innovative exploitation skills and accompanying PED technology improvements. However, enhanced skills and new technology will not automatically provide more cost-efficient PED. Appropriate organizational structure changes are required to successfully leverage ISR manpower and technical capabilities. Now is the time to use existing PED infrastructure to combine ISR capabilities and deliver more than what the Service components can provide individually. The Armed Forces have historically focused on providing intelligence and analysis in direct support of each military Service's core missions. Currently, each Service provides PED of Service-centric sensors with limited joint commonality, little mutual support, and varying implementation concepts (such as reachback, in-theater, and reach-forward PED).

It was originally expected that the DOD DCGS concept would provide a vehicle for standardizing PED competencies across the Services. This would help ensure efficiencies and operational necessity leading to a natural synchronization of best-of-breed ideas, processes, technologies, and organizational structures. It was not foreseen that significant differences in operational requirements would drive each of the Services to focus on separate parts of the intelligence cycle, commonly called PCPAD (planning and direction, collection, processing and exploitation, analysis and production, and dissemination and integration).[2]

The Air Force has concentrated its DCGS capabilities on processing and exploitation with an emphasis on worldwide distributed operations, reachback, and minimizing its in-theater presence and workload. The Army has focused primarily on the analysis and production of accessible information and intelligence previously tagged and cataloged (often referred to as conditioned data or metadata tagged information) with the intent of embedding advanced intelligence analysis capability within combat units. Both the Navy and Marine Corps DCGS concepts, while including PED, emphasize analysis and fusion of intelligence in support of tactical and operational commanders' needs. This is partly driven by having a limited number of sensor systems requiring remote PED. However, as both the Army and Navy increase their inventory and type of airborne ISR systems, overall demand for PED is likely to increase.

Moving Forward Jointly

Uncertainty of future operational situations will force DOD to explore new approaches in the way it manages, processes, and presents ISR data to the warfighter. Increasing PED manpower in existing organizations is not an option in a resource-constrained environment. Instead, some tout advanced technology as providing the path forward. Unfortunately, the successes of social media and Google searches do not translate to automated support for imagery and signals processing under militarily relevant conditions. In reality, technology to solve issues such as automatic change detection and machine-only target recognition to ease PED challenges remains years away. Therefore, DOD needs to continue robust research and development in this area, but it cannot solely plan on technology for near-term success. These challenges, combined with a downsizing force, will drive us toward collocation, integration, and information-sharing. This article discusses another alternative—a single, integrated, joint, coalition, and IC PED construct—DCGS-Future.

As envisioned, DCGS-Future would provide PED for all collection platforms and sensors. It complements the joint intelligence centers, whose mandate includes analysis, collection management, targeting, and other missions focused on a single theater. As one part of a larger, integrated, future ISR enterprise, DCGS-Future would operate across the entire PCPAD cycle with the intent of providing all-source fused intelligence to meet joint warfighter requirements. In this future integrated ISR enterprise, DCGS-Future, Service intelligence elements, the intelligence combat support agencies (CSAs)[3], other IC elements, and coalition partners would deliver foundational intelligence and specialized expertise for incorporation into customer-centric products. A robust capability to process, exploit, and disseminate a wide set of raw ISR data from varied collection platforms and the ability to manage PED capability and capacity across the entire collaborative DCGS enterprise are the core advantages of DCGS-Future.

DCGS-Future would also deliver increased operational effectiveness and cost savings within the realities of declining budgets, changing strategic environment, and technological advances. It recognizes that each Service DCGS was has been driven first by Service needs. DCGS-Future, however, seeks to take advantage of Service-specific specialization and expertise to reduce redundancy and improve overall ISR capability. For example, the Air Force would bring unrivaled imagery processing and metadata tagging and a distributed and federated approach via reachback, while the Army would bring in-depth analysis and fusion, robust linguistic capabilities, and a tactical mindset to the fight. In other words, each Service would bring the best of what it does now to the joint effort, providing real-time joint warfighter support. Admittedly difficult to achieve, this vision of DCGS-Future is long term and represents only part of a larger future ISR enterprise. Fortunately, efforts are already under way to attain it.

Air Force DCGS currently has a worldwide distributed exploitation model with global reachback capability. It is fast, efficient, operational, and proven

Air Force 711th Human Performance Wing behavioral scientist creates slides from video snapshots during demonstration of new enhanced reporting, narrative event streaming tool (U.S. Air Force/Wesley Farnsworth)

in combat over the past decade in Iraq and Afghanistan. Air Force DCGS has also matured the operational integration with the CSAs to collectively share and support both national and joint customers. Additionally, Air Force DCGS has established a burden-sharing arrangement with the United Kingdom (UK) to PED remotely piloted aircraft ISR missions, optimizing the expertise possessed by each partner. This U.S.-UK agreement provides concrete proof of DCGS-Future's feasibility and benefits in a real-world, combat-related environment.

Army DCGS is developing a PED Center of Excellence physically collocated with Air Force DCGS and National Security Agency (NSA) units. This offers the best of Army, Air Force, and NSA PED capabilities in a single location as an initial joint model of DCGS-Future. Additionally, Army, Marine Corps, Navy, and Air Force intelligence leaders are fostering tighter relationships across PED organizations and finding ways together to move closer to the DCGS-Future construct.

Continued Momentum

While these all show great promise, they barely begin to scratch the surface of actions needed to move DCGS-Future to the level required for tangible operational and fiscal gains. In addition to these early efforts, there are several areas ripe for future consideration. The first centers on the actual PED capability of DCGS-Future. Beginning immediately, the Services should make key personnel exchanges between DCGS organizations. The intent is to provide familiarization, an understanding of mission-level, force-unique capabilities and requirements at the tactical level, and to scope follow-on actions at the Service level. Anticipated near-term follow-on actions could include physical collocation of PED components, technical connectivity, and the development of common training standards, qualifications, and certifications for operators and missions.

The second area for continued action targets DCGS-Future management and operations. The concept would work most effectively if the IC PED organizations made their PED capabilities available for tasking via a single universal method such as the Global Force Management Allocation Process. Each Service would understandably want the ability to retain a portion of its PED capability/capacity for Service-specific requirements. However, DCGS-Future would offer the remaining PED capacity for global assignment. The amount and type of PED that each Service contributes to DCGS-Future could vary based on schedule and mission specifics. Regardless, all military PED requires standardizing across the force and needs mechanisms (technical and procedural) to manage DCGS-Future as a single entity while respecting and integrating Service-specific requirements. The joint Air Tasking Order process provides one model for consideration. It highlights the improved level of support and flexibility achieved when this capability is aligned under a single manager. By pooling PED resources in DCGS-Future, common management tools, processes, and

RQ-4 Global Hawk covers intelligence collection capability to support forces (U.S. Air Force/Amanda N. Stencil)

training could significantly improve asset use and operational efficiency.

Work also needs to move forward in formalizing the DCGS-Future concept. Such an effort requires collaboration and action on an agreed-upon, documented vision with guidance and direction at a sufficient level to solidify and guarantee participation. Formalized documentation would include Under Secretary of Defense for Intelligence, Chairman of the Joint Chiefs of Staff and Service-level agreements, funding actions to support common DCGS-Future efforts, and joint concepts of operations. To achieve a viable DCGS-Future, we must base it on a solid foundation of codified and accepted tactics, techniques, and procedures. Implementation of a concept of this magnitude requires strong advocacy across the Services.

Capability enhancement, guidance, funding, and documentation represent the initial actions needed to start down the path toward DCGS-Future. They are, by no means, a complete list of the activities required. While this article focuses on the joint PED portion of DCGS-Future, expanding DCGS as envisioned to include the IC and partner nations requires additional scope and effort. Changing the Service PED paradigms is a large, complex endeavor that will undoubtedly encounter challenges and suffer setbacks. The endgame is a cross-domain, multifunction ISR enterprise designed to make intelligence available at the right place, at the right time, to the right end user, regardless of who collected the data, who processed it, or where it was processed. Optimizing scarce funding and improving combat mission effectiveness make DCGS-Future a logical way forward for current Service capabilities to meet the challenges of the future and fully support the joint warfighter. **JFQ**

Notes

[1] Intelligence Community elements consist of the Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, Air Force Intelligence Surveillance and Reconnaissance Agency, Army Intelligence and Security Command, Marine Corps Intelligence Activity, Office of Naval Intelligence, Department of Energy Office of Intelligence and Counterintelligence, Department of Homeland Security Office of Intelligence and Analysis, Coast Guard Intelligence, Department of Justice Federal Bureau of Investigation National Security Branch, Drug Enforcement Administration Office of National Security Intelligence, Department of State Bureau of Intelligence and Research, and Department of Treasury Office of Terrorism and Financial Intelligence.

[2] See Joint Publication 2-1, *Joint and National Intelligence Support to Military Operations* (Washington, DC: The Joint Staff, January 5, 2012).

[3] Combat support agencies consist of the Defense Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, Defense Threat Reduction Agency, Defense Logistics Agency, Defense Information Systems Agency, and Defense Contract Management Agency.

I Corps senior enlisted leader and U.S. Army–Japan senior enlisted leader test-drive Japanese Type 90 tank at Camp Higashi-Chitose, Japan, on study tour during Yama Sakura 65 (U.S. Army/Chalon Hutson)

I Corps
U.S. Pacific Command's Newest Asset

By Robert B. Brown and Jason N. Adler

We will of necessity rebalance toward the Asia-Pacific region. Our relationships with Asian allies and key partners are critical to the future stability and growth of the region.[1]

In January 2012, the United States redefined its global security priorities with the words above. The changing global environment, signified by the rising political and economic power of Asia, necessitated an adjustment of national strategic goals. On the surface, little may appear changed in a region mostly covered with blue water. Army forces are still in Korea, Japan, and Hawaii. That surface view belies the strategic, operational, and tactical changes that have occurred as the Army's direction has shifted to the Pacific, spearheaded operationally by I Corps.

The U.S. military learned a great deal from the past 12 years of war in Iraq and Afghanistan. Among these lessons was the necessity of joint operations and

Lieutenant General Robert B. Brown, USA, is Commanding General, U.S. Army Combined Arms Center and Fort Leavenworth, Kansas. He commanded I Corps from July 2012 to February 2014. Major Jason N. Adler, USA, is a member of I Corps Commanding General's Initiatives Group.

coordination with unified action partners. Joint Publication 3-0, *Joint Operations*, summarizes the need for joint operations:

To succeed, we will need adaptive and thinking professionals who understand the capabilities their Service brings to joint operations: how to integrate those capabilities with those of other Services and inter-organizational partners to optimize the strength of unified action: and how to organize, employ, and sustain joint forces to provide national leaders with multiple options for addressing various security threats.[2]

In addition to working with joint partners, the U.S. military must collaborate with its unified action partners as it attempts to plan, coordinate, synchronize, and integrate the activities of governmental and nongovernmental entities with military operations to achieve unity of effort.[3]

The I Corps assignment to U.S. Pacific Command (USPACOM) underscores the Army's commitment to the Pacific region. The addition of an assigned Army corps provides a tailorable, scalable, and agile mission command node as well as unique capability sets that add to USPACOM capabilities to prevent, shape, and win in the region. I Corps increases the options available to USPACOM at the tactical and operational levels. After outlining the importance of the Pacific region, this article focuses on the efforts of I Corps as the Army's only corps assigned to a geographic combatant commander and within the larger Army efforts to rebalance strategically, operationally, and tactically.

Global Importance

The Indo-Pacific region spans half the globe and directly influences the U.S. economy and security. The world's three largest economies reside in the USPACOM area of responsibility (AOR), and the area's global economic importance is significant.[4] Eight trillion dollars of annual two-way trade moves through the region. At any moment, one of every two of the world's cargo ships and two of every three ships carrying energy assets are traveling through USPACOM. The area is home to four of the world's most populous countries, seven of the world's largest armies, and five of the seven U.S. Mutual Defense Agreements.[5] Security cooperation with our allies in Australia, Japan, the Philippines, South Korea, and Thailand is regionally important, and the overall security situation in the region has global effects on trade and economic prosperity. These facts alone make a compelling case for the military interest in the Pacific region.

The Marine Corps, Navy, and Air Force have—and will continue to have—huge roles in achieving the goals stated in the 2010 National Security Strategy. The expeditionary capability of the Marine Corps and Navy to project power in littoral areas and promote security in waterways is unmatched. Army forces also provide valuable combat and support capabilities necessary to achieve regional goals. Rather than set the Army and Marine Corps into a competition in the Pacific, regionally aligned Army corps and subordinate units add vital and complementary capabilities to the joint force. Cooperation and collaboration are necessary to increase the interoperability between Army, Marine Corps, Navy, and Air Force forces. Increased security of this vital portion of the world is well worth the effort.

Twenty-one of the 27 Pacific nations with militaries chose army officers, not admirals or air force officers, as their defense chiefs. That choice suggests a security mindset that the United States must recognize as it seeks to deepen relationships and enhance regional security. Even across language barriers, our common profession as army officers serves as a bridge to mutual understanding and respect. Partnership skills developed over the past 12 years with the armies of Iraq, Afghanistan, and fellow coalition forces will enable the Soldiers of I Corps to develop relationships with our partner armies in the Pacific.

Relationships developed between countries during military-to-military engagements and exercises are an important first step in the Army's ability to prevent conflict and shape the region. Exercises build confidence, trust, and interoperability between the U.S. military and our Pacific partners through a consistent regional partnership program. They prevent conflict by demonstrating the capabilities of the U.S. military as a reliable partner, engaged and focused on creating a stable security environment. Military-to-military engagements shape the region by increasing our Pacific partners' ability to provide security and are a visible demonstration of combined strength. The shared experiences ensure that partner nations understand each other's capabilities and systems and have trust in one another before conducting combined operations during a crisis.

U.S. Army Evolving in the Pacific

Designating the U.S. Army Pacific (USARPAC) commander as a four-star general was a major strategic shift in the command structure of the Pacific Army. This change allowed USPACOM to designate the USARPAC as the Theater Joint Force Land Component Command (JFLCC) for the Pacific region. The new mission command architecture added a more robust theater capability for sustainment, communications, and medical support to respond to the range of military operations in the Pacific.

The elevation of USARPAC to a four-star command created an opportunity for I Corps to expand its role in the region. I Corps is the first operational-level headquarters assigned to a geographic combatant commander in the regionally aligned forces concept. This headquarters has completed an operational capabilities assessment, which certifies it to serve as a joint task force headquarters under USPACOM.[6]

At the tactical level, the Army redefined command and support relationships between U.S. Army Forces Command (USFORCOM) and USARPAC units. The 7th Infantry Division and 593rd Expeditionary Sustainment Command now command nine of the Joint Base Lewis-McChord–based brigades, all of which are aligned to the Pacific, thus

Staff briefs I Corps commander during combined arms rehearsal meeting for U.S.–South Korean annual joint/combined command post exercise Ulchi Freedom Guardian (DOD/Daniel Schroeder)

enabling I Corps to maintain a mission focus on the Pacific. As the operational arm of USARPAC, I Corps now has operational control of the 25th Infantry Division, a coordinating relationship with U.S. Army Alaska and U.S. Army Japan, and operational control of the Alaska-based brigades for missions outside of Alaska.

Strategic, operational, and tactical changes to the mission command structure in the Pacific allow I Corps to provide an operational planning capability, reduce headquarters redundancy, and provide sound three-star level solutions to USARPAC and USPACOM.

A Multi-Echelon Headquarters

An Army corps headquarters provides a scalable, tailorable, and agile mission command node that has the capability to respond to crises of varying size and duration. The headquarters can tailor and scale itself to the appropriate size and capability set based on the situation. To illustrate that point, elements of I Corps participated in six major exercises in 2013. Three of the six exercises are of particular note as they challenged the corps headquarters to execute operations as a Combined Force Land Component Command (CFLCC), traditional U.S. Army corps, and JFLCC.

In July 2013, I Corps participated in Exercise Talisman Saber with our Australian counterparts in the 1st Australian Division and U.S. Third Fleet, with its Seventh Fleet as the higher headquarters. I Corps deployed its early entry command post (EECP) scaled and tailored to serve as the CFLCC, and it was during this exercise that the headquarters executed its joint task force certification. Admiral Samuel Locklear, commander of USPACOM, noted that I Corps was a "tailorable, agile, operational headquarters ready for deployment across the spectrum of operations."[7]

During this exercise, I Corps provided mission command to two U.S. National Guard Divisions, the Australian 1st Division, the 3rd Marine Expeditionary Brigade, and the 4th Brigade (Airborne) of the 25th Infantry Division. These units were operating in Phases II, III, and IV across a noncontiguous area of operations that stretched the same approximate distance as Iraq to Afghanistan. Of particular note, over 400 paratroopers in five C-17s flew 15 hours straight from Joint Base Elmendorf-Richardson, Alaska, and conducted a joint forcible entry operation north of Rockhampton, Australia. This strategic airdrop demonstrated the ability of a joint and multinational force to project power from the U.S. mainland to anywhere in the Pacific region.

Shortly after Talisman Saber, I Corps participated in Exercise Ulchi Freedom Guardian in August 2013. I Corps deployed a smaller EECP scaled and tailored for service as a traditional U.S. Army corps under the Third Republic of Korea Army. I Corps faced a decisive action scenario complex in its requirements for combined and joint major combat operations, which ensured that the corps is capable of effectively and efficiently operating at the highest end of the range of military operations.

Always learning and growing, I Corps participated in Exercise Yama Sakura 65 in December 2013 alongside our partners, the Japan Ground Self-Defense

U.S. Army Pacific chief of staff welcomed 39 senior leaders participating in U.S. Army War College International Fellows program to Fort Shafter, Hawaii (U.S. Army/Kyle J. Richardson)

Force. In this exercise, the corps deployed a robust EECP scaled to 400 of the corps staff and 50 Reserve and joint augmentees, and integrated the I Corps (Forward)/U.S. Army Japan commander as a deputy commanding general. The corps tailored itself to operate as a JFLCC alongside Japan's Ground Self-Defense Force Northern Army. This unique bilateral environment, coupled with the exercise's unified action complexity, put a premium on building a cohesive team, creating shared understanding, and developing mutual trust.

Through exercises such as Talisman Saber, Ulchi Freedom Guardian, and Yama Sakura 65, I Corps has proved itself as a headquarters that offers operational solutions to USARPAC and USPACOM commanders. Significantly, a corps headquarters, certified as a joint task force and with recent operational-level experience in Afghanistan, provides these commanders with a headquarters capable of conducting mission command in any situation and in various command capacities within the Pacific region.

Unique Capabilities

The regional alignment of an Army corps and subordinate units gives a tremendous amount of flexibility to the USPACOM commander to be able to support the entire range of military operations. Regionally aligned forces execute theater security cooperation activities, bilateral and multilateral military exercises, and operations support. They provide the combatant commander with forces that can respond to crises and have the necessary language capability and regional expertise.

The realignment of command and support relationships between I Corps, 25th Infantry Division, U.S. Army Alaska, and U.S. Army Japan brings an amazing amount of capability to the Pacific. In addition to the two organic Stryker brigades, I Corps now has four additional brigade combat teams at its disposal for contingency operations. These maneuver brigade combat teams bring more depth to the already robust amount of land combat power resident in the U.S. Marine Forces Pacific.

Perhaps more importantly, Army assets such as aviation, engineer, civil affairs, military police, surveillance, logistics, communications, and medical will provide critical expertise and capabilities during contingency operations. The addition of these U.S. Army resources to elements already resident in the Pacific will allow USPACOM to respond to any contingency for an extended duration with the numbers and types of tools needed for success.

Pacific Pathways

USARPAC developed a new concept called Pacific Pathways that supports both regional operational contingencies and tactical training needs. Army forces operating in the region will be able to collaborate with Pacific partner military forces for training and be responsive to developing crises. Pacific Pathways supports the current engagement strategy of "assure, promote, enhance, open, sustain," and puts the most highly trained units closest to potential crisis.[8] The I Corps role in executing Pacific Pathways is to provide training and

Indonesian National Armed Forces and U.S. Army Soldiers receive tactical briefing during field training exercise Garuda Shield 2014 (U.S. Army/Matthew Veasley)

readiness authority over units executing Pathways, to resource solutions for USARPAC, and to mission command the units executing Pathways.

In July 2014, a single Joint Base Lewis-McChord Stryker brigade combat team conducted a Pathways proof of principle. The unit chosen to execute the first Pacific Pathways mission was one of the seven brigades of the Army Contingency Force. Its selection was a deliberate decision to dedicate a unit at the highest state of readiness toward the rebalance to the Pacific. The brigade task-organized to accomplish the objectives of the major exercises, facilitated continued military-to-military engagements in the Pacific region, and provided rapidly deployable options for USPACOM in response to emerging situations. The task force elements were a mission command headquarters (battalion or brigade), tactical force, aviation, support, and enabling elements.[9]

Under the Pacific Pathways concept, a brigade will spend 2 to 3 months in the USPACOM AOR following a combat training center rotation. Once the Pathways mission begins, the 25th Infantry Division will assume mission command of the brigade for the duration of the three exercises and for any contingency operations. After it has completed its Pathways missions, this highly trained unit will then be available to USPACOM to respond to emerging contingency operations in the Pacific.[10]

Leader Development

I Corps recognizes that a major challenge to operating in such a vast region is the development of long-term, meaningful relationships with our Pacific security partners. Annual exercises and the Pacific Pathways initiative are examples of efforts to prevent and shape in the Pacific, and they are opportunities to build and maintain critical relationships. The development of leaders capable of executing at the operational and strategic levels is the goal of the I Corps plan. These leaders must have the language and the regional expertise to understand the geopolitical context of the operating environment, and they must integrate with unified action partners in government, nongovernmental agencies, and our Pacific military partners.

It is to that end that I Corps created a biannual Senior Leader Development Training program for our military senior leaders and leaders from our Pacific partner nations. The most recent 2-day event focused on organizational leadership and humanitarian assistance/disaster relief. Partner agencies included the Army, Navy, Air Force, Army National Guard, Reserve, Coast Guard, U.S. Agency for International Development, and the Japan Ground Self-Defense Force. Executives from Microsoft, Northrop Grumman, Boeing, Amazon, and the American Red Cross also contributed to

the training experience. This diverse audience generated thoughtful discussions and built cross-organizational relationships as they grappled with the issues, developed a better understanding of alternate perspectives, and learned from shared experiences.

Efforts to build tactical expertise in the Pacific region have not stopped with leader development training. I Corps and I Marine Expeditionary Force are also planning to co-host the Land Power in the Asia-Pacific workshop, which will examine the role of ground power in America's rebalance to the Pacific. Through presentations, panel discussions, and breakout groups, senior Army and Marine Corps leaders will develop a shared understanding of the role for land power in the region. The workshop will specifically focus on the Asia-Pacific security environment, capability requirements, and the challenges to rebalance.

In addition, the Joint Base Lewis-McChord Language and Culture Center is a valuable resource for I Corps leaders to assist them in understanding the human domain of the Pacific region. It provides language, regional expertise, and culture training designed to equip Soldiers with mission-critical language and cultural information. Commanders prepare themselves and their units for intercultural interactions by selecting from a full range of language and culture training. Training tailored to specific mission requirements includes facilitated or self-paced cross-cultural communication classes, language familiarization courses, culture-specific training, and area orientation briefings. I Corps leaders recognize the operational benefits stemming from language and culture training as a way to enhance their unit's ability to communicate across cultures. They also appreciate the importance of the human aspect of operations within the Pacific region as a means to build lasting relationships with our Pacific partners and bolster regional security.

Conclusion

Through the joint warfighting capability, along with our unified action partners, the U.S. military is postured to provide security force assistance and contingency support to its Pacific partners. Considering that the USPACOM AOR makes up nearly one-half of the entire world, it is necessary that all Services be brought together to amplify their respective capabilities. The effective mixture of the Army, Marine Corps, Navy, Air Force, and capabilities in USPACOM is truly an amazing and unmatched effort to achieve national strategic goals in the region.

As part of the rebalance to the Pacific, the Army has made strategic, operational, and tactical adjustments to the regional mission command architecture. The elevation of USARPAC to four-star status, regional alignment of I Corps to the Pacific, and realignment of the subordinate command structure signify the Army's commitment to the region. The additional Army functional and multifunctional brigades lend depth to the capabilities long resident in the Pacific.

Finally, the certification of I Corps as a joint task force capable of executing mission command as an Army corps, Combined or Joint Force Land Component Command, or joint task force gives the combatant commander more options when responding to crises in the Pacific. Rather than set the Services into a competition, the additional Army capabilities are complementary to those already in the region and enhance the military's ability to accomplish the security priorities laid out by the President in January 2012. **JFQ**

Notes

[1] *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: Department of Defense, January 2012), available at <www.defense.gov/news/Defense_Strategic_Guidance.pdf>.

[2] Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: The Joint Staff, August 11, 2011), 1, available at <www.dtic.mil/doctrine/new_pubs/jp3_0.pdf>.

[3] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, as amended through December 15, 2014), 276, available at <www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>.

[4] U.S. Pacific Command, "USPACOM Facts," available at <www.pacom.mil/about-uspacom/facts.shtml>.

[5] U.S. Army Pacific (USARPAC), "U.S. Army Land Power in the Pacific," available at <www.afcea.org/events/tnlf/east12/documents/MathewsRevRecvd.pdf>.

[6] JP 3-0, IV-7.

[7] Admiral Samuel Locklear, "Talisman Saber After Action Review," speech, Northampton, Australia, July 27, 2013.

[8] USARPAC Information Paper, "Pacific Pathways—An Army in Motion," November 22, 2013, 7.

[9] Ibid., 4.

[10] Ibid., 5.

President Obama talks with Russian President Vladimir Putin about situation in Ukraine, March 1, 2014 (White House/Pete Souza)

The Military's Role in Rule of Law Development

By Patrick J. Reinert and John F. Hussey

America's commitment to the rule of law is fundamental to our efforts to build an international order that is capable of confronting the emerging challenges of the 21st century.

—President Barack Obama[1]

Brigadier General Patrick J. Reinert, USAR, is a career Assistant United States Attorney in the Northern District of Iowa. Colonel John F. Hussey, USA, is Deputy Commander of Combined Joint Interagency Task Force 435 in Afghanistan.

As Operation *Enduring Freedom* in Afghanistan transitions to the Resolute Support Mission, many believe that military engagements abroad involving the United States will decrease and that the Nation will become a disengaged actor on the world stage. Given the complexity and volatility of relationships among nations, however, as well as the continual rise of hostile transnational groups, it appears the United States will remain

substantially engaged on the international stage for the foreseeable future. As part of its future engagement strategy, the United States must consider and plan for conducting operations in states at risk of failure, in failed states where the central government is so weakened that the people have virtually returned to the natural state described by Thomas Hobbes in the *Leviathan*, in states emerging from long periods of conflict such as Afghanistan, and in states in peaceful postconflict rebuilding periods.[2]

The world remains a volatile, uncertain, and dangerous place with states, transnational organizations, and nonstate actors all working in their own self-interests—which may or may not be aligned with the national interest of the United States. There is little choice for the United States but to maintain an active role to counter, impede, and dissuade hostile states, nonstate actors, and transnational criminal organizations. The United States, working in concert with other nations, international organizations, and nongovernmental organizations (NGOs), must work to mitigate threats through the use of all elements of national power and focus on rule of law development as a means to provide international stability.

If combat operations are required to wrest control of a nation or a large geographic area from a hostile force or if a nation becomes a failed state requiring international intervention, each participating nation must plan for and be prepared to implement programs to provide security and stability. Using as much of the indigenous criminal justice system as soon as possible should protect the people from harm and help them begin developing a sense of "nation" to form the nucleus of the nation that will rise from the ashes of the conflict. Rule of law development requires a whole-of-government approach in which synchronization and coordination among the military, Embassy teams, international organizations, and NGOs are critical. In an operation with a kinetic component, or where the security situation may be unstable, the military must take the lead in developing the security umbrella using the criminal justice system for counterinsurgency and providing general security for the people. Other rule of law programs, focusing on more generalized development efforts, have a longer time horizon and can more effectively flourish after the security situation is more stable.

David Kilcullen, former counterinsurgency advisor to General David Petraeus in Iraq, stated the United States is likely to remain engaged in major stabilization or counterinsurgency operations such as Iraq or Afghanistan.[3] In a world of uncertainty and instability, Kilcullen predicted the United States will engage in smaller operations, such as those in Bosnia or Kosovo, every 5 to 10 years for the foreseeable future.[4] These conflicts will likely occur in conflict-ridden littoral areas and in underdeveloped regions of the Middle East, Africa, Latin America, and Asia.[5] Operational planners must anticipate that coalition military forces and international organizations will confront failed, broken, or simply nonexistent justice systems that lack sufficient capability or capacity to conduct law enforcement operations, effectively resolve civil or criminal disputes, or appropriately conduct detention operations to support Law of Armed Conflict (LOAC) or criminal detentions in accordance with international humanitarian standards.[6]

What Is Rule of Law?

The rule of law has been described in varying terms, but a comprehensive definition, such as the one used by the United Nations, is useful in this context. The United Nations defines *rule of law* as:

a principle of governance in which all persons, institutions and entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness and procedural and legal transparency.[7]

Many nations use secular constitutions, statutes, and mechanisms (law enforcement, courts, and institutions to correct individual criminal behavior) to implement rule of law. Other nations use differing implementation methods. In the Middle East, for example, the structure of the legal system is derived from a combination of systems, including religion and tribal practice, to form formal and informal legal mechanisms. In Latin America, citizens believe that they do not have a voice or the ability to obtain justice from a system permeated by corruption, judicial failures, repressive police tactics, and the legal marginalization of the majority of the population.[8] Citizens in Central Asia, most notably the Caucusus states, assume that they are governed by institutions that are inept, corrupt, and rife with nepotism.[9] In some parts of the world, rule of law appears under the guise of a strong authoritarian ruler exercising great influence over the "independence" of the judiciary. Often rulers with a strong "law and order mentality" impede social change that may threaten their holds on power. In states with a strong Islamic influence, personal issues, such as divorce and marriage, are resolved in sharia courts. The judges in criminal courts may be educated to approach criminal matters differently than judges trained in sharia law.[10]

For those who have deployed to or are familiar with war-torn areas or failed states, it is clear that military force alone will not be able to establish or implement rule of law. Legal systems and institutions take years to develop based on a variety of factors, including host nation culture, religion, and tolerated levels of corruption, and whether coalition members bring with them an ethnocentric bias that could complicate the establishment of rule of law. In at-risk, failed, emerging, and postconflict states, the military can set the conditions for rule of law development and stability by focusing on the state's criminal justice system.

Afghan National Army soldiers stand in formation outside Bagram Air Field as part of ceremony giving Afghan government control of local prison (U.S. Army/Andrew Claire Baker)

Rule of Law in Afghanistan

After the Taliban government fell in Afghanistan, extremist organizations and insurgents continued to wage asymmetric warfare. The United Nations Security Council through the North Atlantic Treaty Organization (NATO) established the International Security Assistance Force (ISAF) to oversee security in the country. Under ISAF, a new sovereign national structure developed in Afghanistan in 2004. This new government faced significant challenges in establishing rule of law in a country that had been a battleground for years and was still a kinetic environment.

In much of Afghanistan, the legal system struggled to provide stability for the nation due to overly bureaucratic institutions focusing on central control; a traditional preference for local, informal dispute resolution; and a security environment challenging justice actors to maintain a regular presence in some areas, resulting in a virtually nonexistent formal criminal justice system. This allowed the Taliban to fill the void with shadow courts using a rough variant of sharia law. Continued instability and the lack of significant economic growth have caused Afghanistan to struggle with sustaining required infrastructure and trained personnel to maintain rule of law institutions in the short term.

As noted in a recent RAND study, military planners and policymakers repeatedly treated detention operations as an afterthought. Detention operations have had strategic consequences for the United States internationally since 2001.[11] Planning and resourcing detention operations and rule of law development in the earliest phases of the campaign create additional challenges in conducting counterinsurgency operations. Although the international community was quick to offer solutions to address Afghan institutional shortcomings, real reform of the justice system required an Afghan system to ensure protection of civil liberties, equal treatment, and stability. To conduct effective counterinsurgency operations, Afghans needed a trusted criminal justice system void of corruption and abuse of power. In 2009, the U.S. Embassy in Kabul and ISAF commander recognized the need for coordination of military and civilian rule of law efforts.

A Response to the Dilemma

In addition to a struggling judicial system, Afghanistan had a prison system that focused on the provincial rather than national level, resulting in detainees being removed from the battlefield and taken to a court in the same war-torn province. This process placed the provincial legal system at higher risk of

attack and illegal influence. The LOAC detention system used by the coalition was not part of the civilian system, and Afghanistan preferred using criminal procedure rather than administrative detention. Major General Douglas Stone, former Task Force 134 commander in Iraq, came to Afghanistan to review the Afghan prison system. His report was critical of coalition detention operations and found that approximately two-thirds of the detainees were not hardened radicals. Some were not involved with the insurgency, and others worked for the insurgency out of economic necessity.[12] General Stone felt detention centers and prisons should be rehabilitative in nature, which required separating insurgents from common criminals. This seminal report led to change.

On July 9, 2009, ISAF Commander General Stanley McChrystal requested approval to establish Joint Task Force (JTF) 435 to centralize detention operations, interrogation, and rule of law functions in Afghanistan while reducing strategic vulnerabilities posed by detention operations. On September 18, 2009, the Secretary of Defense established JTF 435 to assume command, control, oversight, and responsibility for all U.S. detainee operations in Afghanistan. JTF 435 assumed responsibility from Combined Joint Task Force 82 for the detainees held at the Detention Facility in Parwan (DFIP), oversight of detainee review processes, programs for the peaceful reintegration of detainees into Afghan society, and coordination with other agencies and partners for the promotion of the rule of law and biometrics in Afghanistan. JTF 435 achieved initial operations capability on January 7, 2010.

JTF 435 coordinated with a variety of military and civilian organizations, including Afghan organizations. In addition to the Kabul headquarters element, the JTF had seven subordinate elements:

- Military Police brigade maintaining humane custody, care, and control of detainees, limiting insurgent activity within the facility, and facilitating family visitation
- Theater Intelligence Group (TIG) to collect actionable intelligence
- Biometrics Task Force to confirm identities, track offenders, and build a biometric database
- Afghan Detentions and Corrections Advisory Team (later called the Security Forces Assistance Team) to coordinate with Afghan detention authorities and share best practices
- strategic communications and outreach cell to advance rule of law
- reintegration cell to facilitate deradicalization and reentry programs for Afghan prisoners
- Legal Operations Directorate to conduct periodic Detainee Review Boards and facilitate transfer of detainees to the Afghan criminal courts.[13]

With the addition of Afghan and interagency partners, JTF 435 became Combined Joint Interagency Task Force (CJIATF) 435 on September 1, 2010. The command also assumed new missions and responsibilities to support rule of law efforts as it partnered with the U.S. Ambassador to Afghanistan for Rule of Law and Law Enforcement. To effectively execute rule of law missions, CJIATF 435 created the Rule of Law Field Force–Afghanistan (ROLFF-A) to execute projects to increase rule of law capacity in Afghanistan.[14] The concept required the Embassy and ROLFF-A to concur on programs to build short-term, mid-term, and long-term Afghan governance and justice systems. ROLFF-A then coordinated with battlespace owners to build capacity of local legal systems to allow them to operate effectively across the legal spectrum. ROLFF-A, in conjunction with U.S. law enforcement agencies, provided subject matter experts on evidence-processing to assist Afghan prosecutors and investigators.

On June 9, 2011, the defense ministers from the 48 nations of ISAF created the NATO Rule of Law Field Support Mission (NROLFSM) as a command directly subordinate to the ISAF commander. The commander of ROLFF-A was also the NROLFSM commander. NROLFSM provided essential field capabilities for Afghan and international civilian providers to build Afghan criminal justice capacity, increase access to dispute resolution services, fight corruption, and promote the legitimacy of the Afghan government by providing security, coordination, movement support, engineering support, and contract oversight.

Under the ROLFF-A/NROLFSM mandate, U.S. Rule of Law Field Support Officers, predominantly lawyers and law enforcement officials, mentored justice sector officials.[15] Neither ROLFF-A nor NROLFSM were to participate in U.S. LOAC detention operations.[16] To be successful in a geographically dispersed rule of law mission, a unit such as ROLFF-A/NROLFSM needs to be well resourced and able to operate for an extended period of time. For future military forays into rule of law, a more focused effort is warranted.

In today's complex battlefield, military leaders have come to realize that achieving national goals to transition from combat to stability operations and ultimately transfer to host nation civil authority requires rule of law planning and shaping efforts well before combat operations. To facilitate the eventual transition to the host nation, rule of law planning must include incorporation of significant aspects of the host nation's legal system. The military rule of law plan must create the security umbrella and focus on criminal justice basics, specifically detentions, investigations, and adjudications. The military's use of these universal components of a criminal justice system must be as close as possible to the host nation's legal system to enable effective transition to host nation sovereignty. Military rule of law planning must focus on the basic security institutions to create a permissive environment for the interagency community, NGOs, and coalition partners to operate.

One of the primary goals of CJIATF 435 was to assist its Afghan partners in establishing a detention operations regimen, a detainee interview process to enable them to continue to gather information for prosecution and network targeting, and a court to adjudicate charges of criminal activity by members

of the insurgency. The commander's vision was "to build Afghanistan's resistance and resiliency against insurgent and terror-related threats through use of evidence-based operations, forensic evidence, and enhanced cooperation across the Afghan Justice Sector."[17] In an effort to build the Afghan legal system and transition this facet of the operation to the Afghans, CJIATF 435 focused its mission on training the Afghan partners in detentions, interview techniques to perfect criminal cases, and court operations to resolve criminal cases related to the insurgency.

Investigations

To dismantle any criminal network, investigators must gather information to understand the network, methods of operation, identity of participants, and their roles. One of the important methods to gain insight into a criminal network is the interview of a suspect. In conducting operations against a networked adversary such as an insurgent group, an interview can result in information to conduct future operations to disrupt or dismantle the network on the battlefield while simultaneously obtaining evidence to use against the individual in the host nation court system. In Iraq, the model used to conduct detainee interviews was the Joint Intelligence and Debriefing Center.[18] In Afghanistan, the Theater Intelligence Group and its Afghan partner, the National Directorate of Security, Department 40 (NDS-40), filled this role.

The TIG was created on January 6, 2010 and was assigned to CJIATF 435 to conduct interviews and debriefings to fill tactical, operational, and strategic intelligence requirements. Eventually, the TIG had more than 300 Servicemembers, civilians, contractors, and linguists assigned and forged working relationships with more than 20 interagency partners and organizations.[19] The TIG conducted more than 35,000 interviews and debriefings and produced over 6,800 reports supporting all echelons of intelligence consumers.[20] In 2013, the TIG began partnered operations with law enforcement investigators from NDS-40, which investigates individuals suspected of committing crimes in support of the insurgency. In this partnership, NDS-40 investigators were able to hone their skills at using forensic evidence, map tracking, and other interview techniques taught by the U.S. mentors in the TIG.

Court Operations

The evidence gathered through this joint effort enabled the Afghan legal system to remove insurgents from the battlefield. CJIATF 435 worked with the U.S. Department of State, international partners, and Afghan officials to develop the Justice Center in Parwan (JCIP) in 2010.[21] The concept was for Afghans to have an effective, centralized criminal court to resolve national security–related cases applying Afghan law. The JCIP was to be a long-term facility led by Afghan judges, prosecutors, and defense counsel and was collocated with the Afghan National Detention Facility in Parwan (ANDF-P) within the National Security Justice Center (NSJC).[22] At the JCIP, every detainee had a dedicated defense counsel, and justice advisors from other countries assisted counsel in honing their advocacy skills and effectively presenting cases before the court.

From May 2010 through September 2014, the JCIP provided due process to over 3,000 detainees through an Afghan criminal court operated by Afghan judges applying Afghan law. The JCIP successfully conducted over 7,000 primary and appellate trials of insurgents removed from the battlefield.[23] The legal advisors reviewed and reported the results of the majority of JCIP trials to help improve the process and capture lessons learned. The court maintained an overall conviction rate of over 75 percent and a conviction rate of 98 percent if there was DNA or a fingerprint match to an improvised explosive device.[24] The court's application of Afghan criminal law, specifically the Internal/External Security Crimes Act, effectively protected the coalition and the Afghan people. The JCIP provided a sustainable foundation for Afghanistan to effectively implement Afghan law to criminalize the insurgency and build the people's confidence in the national government and legal system. The effective prosecution at JCIP creates a beacon of hope for the rest of the criminal justice system in the eyes of the Afghan people. Furthermore, an effective National Security Justice Center also counters the narrative that Afghanistan is the source of regional instability.

Detentions

As with Iraq and Guantanamo Bay, detention operations in Afghanistan had a variety of challenges. The original detention facility in Afghanistan, the Bagram Collection Point, later called the Bagram Theater Internment Facility, was challenged by a variety of issues, including the facility design. In 2009, the Detention Facility in Parwan was constructed with a view to transition detention operations to Afghan authority.[25] By the end of 2010, 561 Afghan guards had been trained to work at DFIP. Also, CJIATF 435 trained and mentored Afghan leaders to prepare them to assume responsibility for legal processing, case management, and administrative/logistical operations of the detention facility. CJIATF 435 facilitated the creation of the Afghan Military Police Brigade, a 5,294-man unit specially trained to conduct detention operations in accordance with international humanitarian standards.[26]

CJIATF 435 transferred DFIP and the Afghan detainees to the control of the Afghan government on March 9, 2012, and the facility was renamed the Afghan National Detention Facility in Parwan.[27] The Afghan Military Police Brigade, subsequently designated the Detention Operations Command, remained part of the Afghan National Army and maintains control over the ANDF-P. The ANDF-P, JCIP, and support bases collectively constitute the NSJC. CJIATF 435 continues its partnership with the Afghan National Army, NDS-40, the court, prosecutors, and defense counsel to support the justice sector in combating the insurgency and creating a more stable Afghanistan.

Governing Ungoverned Territory

In the near term, the challenge for the United States is remaining globally engaged with limited resources. After nearly 13 years of continuous conflict in Iraq and Afghanistan, the United States and its coalition partners are war-weary. The duration of the conflicts, coupled with economic issues at home, makes domestic issues a focal point for politicians eager to avoid military engagements. To support global stability and prevent ungoverned territory from becoming a safe haven for extremist groups, the United States and its allies must carefully select the means to achieve the strategic goal of preventing nations from becoming failed states while avoiding long-term military engagements. This entails providing assistance to nations that are confronting destabilizing nonstate actors and transnational criminal organizations.

To achieve this objective, the United States and like-minded allies must concentrate on rule of law–focused engagement through routine military and interagency activities in an effort to dissuade or deter potential adversaries while solidifying relationships with friends and allies. These engagements will influence and strengthen the leadership of a nation and its populace. This engagement strategy requires a coordinated effort among the Defense Department, State Department, and other governmental agencies to formulate a holistic plan to help a nation or region avoid slipping into disunion and to enhance the ability of the nation to govern its territory. In many instances, this will require individuals on the ground to help build the legal institutions necessary for stability. The military is well suited to provide training in a less permissive environment to build security, stability, and a host nation's forces to enhance rule of law and reduce the risk of instability. Reinforcing or reforming a nation's security, prosecutorial, and judicial institutions helps create the fabric of a safe society functioning under the rule of law, while creating a more permissive environment for nonuniformed personnel to establish more long-term development programs.

California National Guard Special Forces Soldier trains with Nigerian soldier in Nigeria to assist local military to counter Boko Haram (DOD/Jason Sweeney)

While it may be more efficient to conduct training in detention operations, investigations, and legal operations in an academic environment in the United States, this method should be limited to key leaders identified during training occurring in the host nation. The bulk of training events must occur in the host nation. This allows trainers to gain a better understanding of the host nation's legal system and culture while identifying key current and future leaders for additional training outside the host nation. Training like that conducted by the Defense Institute of International Legal Studies is an excellent example of rule of law development training conducted in the host nation.[28]

All training must be tailored, focused, and incorporate the local legal system. Attempting to impose a new Western system or to make drastic changes to the existing legal framework will meet with resistance and undermine training efforts, which should focus on compliance with international humanitarian standards. This focus improves the professionalism of the force and mitigates the risk

KC-10 Extender refuels F-22 Raptor over undisclosed location before targeted airstrikes in Syria to protect U.S. personnel from Islamic State in Iraq and Levant (DOD/Russ Scalf)

posed by an abusive authority figure to the rule of law. Abusive, predatory, or corrupt public officials undermine the legitimacy of the government in the eyes of the people. Police forces must enforce the law fairly and equally without regard for status, tribal/ethnic affiliation, or personal gain. In a nation emerging from conflict or striving to maintain legitimacy, the training must initially focus on the three necessary components for a functioning rule of law system: investigation, adjudication, and detention.

Investigations training must focus on basic investigative skills and human rights training to ensure international humanitarian standards are met. In some nations, the police will be responsible for the interview of alleged criminals/insurgents. Trainers must ensure any interview techniques comport with international humanitarian law. Any indigenous interview methods in the host nation that could result in a coerced statement must be specifically discouraged and the negative ramifications of such illegal activity discussed during the training.

The area of detentions is critical to establishing or preserving the rule of law. As noted by the classic Russian writer Fyodor Dostoevsky, "Humane treatment may raise up one in whom the divine image has long been obscured. It is with the 'unfortunate,' above all, that humane conduct is necessary."[29] Without enlightened detention policy and rehabilitative programs, a detention center or prison can easily become a breeding ground for insurgents or other criminals. A poorly trained, corrupt, or abusive guard force will result in detainee abuse, causing the detainee to leave the facility a worse criminal than he entered. Detention and prison officials must understand their role is simply ensuring the safe and humane care of detainees in their custody. If a detainee or prisoner is humanely treated and given constructive rehabilitative training opportunities, the detention center can help create positive change in his behavior.

A free, impartial, and independent legal system, which ensures equal protection under the law and provides due process, is critical to the stability of a nation. The host nation may have a tradition of informal dispute resolution, such as allowing a village elder to resolve disputes, or a more formal legal structure. Informal methods are best suited for resolving individual, civil disputes, such as a land boundary dispute between neighbors. The formal mechanisms are best suited for resolution of criminal matters where the state is taking action to ensure the people are protected from criminal elements. To maximize the ability of the host nation to maintain security, initial training and development efforts should focus on the formal legal mechanisms, specifically the courts and counsel. The three rule of law building blocks of investigation, adjudication, and detention form the security foundation for the nation.

A failed, emerging, or postconflict nation is challenged to provide basic services such as garbage collection and water distribution; performing even basic government services is dependent upon first establishing security. Effective legal institutions are critical to establish and maintain rule of law by creating an environment for the rest of society to flourish. It is in the interest of the United States and the community of nations to ensure the stability of nations, minimize the number of failed states, and help emerging states become stable members of the international community. Using military rule of law development and training teams focused on investigation, formal adjudication, and detention should promote stability, reduce the risk of a failed state, and create the umbrella of security needed for other societal development. This military doctrinal focus should result in a narrow rule of law mission for the military to conduct in a kinetic environment, a clear line of demarcation from civilian development programs, and enhanced synchronization of rule of law development efforts. **JFQ**

Notes

[1] *National Security Strategy* (Washington, DC: The White House, May 2010), 37, available at <www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>.

[2] Ross Harrison, *Hobbes, Locke, and Confusion's Masterpiece: An Examination of Seventeenth Century Philosophy* (Cambridge: Cambridge University Press, 2003), 70.

[3] David J. Kilcullen, "The City as a System: Future Conflict and Urban Resilience," *The Fletcher Forum of World Affairs* 36, no. 2 (Summer 2012), 20, available at <www.fletcherforum.org/wp-content/uploads/2012/09/Kilcullen.pdf>.

[4] Ibid., 22.

[5] Ibid., 34.

[6] John F. Hussey with Larry W. Dotson, "Seizing the Initiative by Establishing the Rule of Law During Combat Operations," *Military Review*, January–February 2013, 30, available at <http://usacac.army.mil/CAC2/MilitaryReview/repository/MilitaryReview_201302280001-MD.xml>.

[7] United Nations Security Council, *The Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies: Report of the Secretary-General* (S/2004/616), August 23, 2004, available at <www.unrol.org/files/2004%20report.pdf>.

[8] Hugo Frühling, "A Memorandum on the Rule of Law and Criminal Violence in Latin America," 3, available at <www.princeton.edu/~piirs/projects/Democracy&Development/papers/Panel%20IV%20Fruhling.pdf>.

[9] Brent T. White, "Putting Aside the Rule of Law Myth: Corruption and the Case for Juries in Emerging Democracies," *Selected Works of Brent T. White*, available at <http://works.bepress.com/brent_white/1/>.

[10] Lionel Beehner, "Religious Conversion and Sharia Law," *Backgrounder*, Council on Foreign Relations, June 8, 2007, available at <www.cfr.org/malaysia/religious-conversion-sharia-law/p13552>.

[11] Cheryl Benard et al., *The Battle Behind the Wire: U.S. Prisoner and Detainee Operations from World War II to Iraq* (Santa Monica, CA: RAND, 2011), available at <www.rand.org/pubs/monographs/MG934.html>.

[12] *The Report of the Constitution Project's Task Force on Detainee Treatment* (Washington, DC: The Constitution Project, 2013), 76, available at <http://detaineetaskforce.org/pdf/Full-Report.pdf>.

[13] John H. Modinger and Joseph T. Bartlett, "A History of Detainee Operations in Afghanistan: How Combined Joint Interagency Task Force 435 Came to Be and What It Has Done," July 1, 2012, unpublished paper in authors' possession, 27–28.

[14] See Rule of Law Field Force–Afghanistan, "Rule of Law Support Mission History and After Action Review," approved by Brigadier General Patrick J. Reinert, on file at The Judge Advocate General's Legal Center and School, Center for Army Lessons Learned, and the Army Center for Military History.

[15] Rule of Law Field Force–Afghanistan, *Rule of Law Field Support Officer Deskbook* (Brussels: NATO Rule of Law Field Support Mission, 2012), 21.

[16] Memorandum for the Under Secretary of Defense (Policy), Pentagon, Washington, DC, from General David Petraeus, December 10, 2010.

[17] Commander, Combined Joint Interagency Task Force (CJIATF) 435 Vision Statement.

[18] Thomas R. Mockaitis, *The Iraq War: A Documentary and Reference Guide* (Westport, CT: Greenwood, 2012), 222.

[19] Modinger and Bartlett, 43–44.

[20] Ibid., 44.

[21] *Report on Progress Toward Security and Stability in Afghanistan* (Washington, DC: Department of Defense, April 2012), 75, available at <www.defense.gov/pubs/pdfs/Report_Final_SecDef_04_27_12.pdf>.

[22] Modinger and Bartlett, 38.

[23] CJIATF 435 records as of September 2014; also see S. Res. 355, 113th Cong., 2nd sess., available at <www.congress.gov/bill/113th-congress/senate-resolution/355/text>. The Justice Center in Parwan has a conviction rate of roughly 80 percent. See David Pendall and Cal Sieg, "Biometric-Enabled Intelligence in Regional Command–East," *Joint Force Quarterly* 72 (1st Quarter, January 2014), available at <http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/8327/jfq-72-biometric-enabled-intelligence-in-regional-command-east.aspx>; and *Progress Toward Security and Stability in Afghanistan* (Washington, DC: Department of Defense, April 2014), available at <www.defense.gov/pubs/April_1230_Report_Final.pdf>.

[24] Ibid.

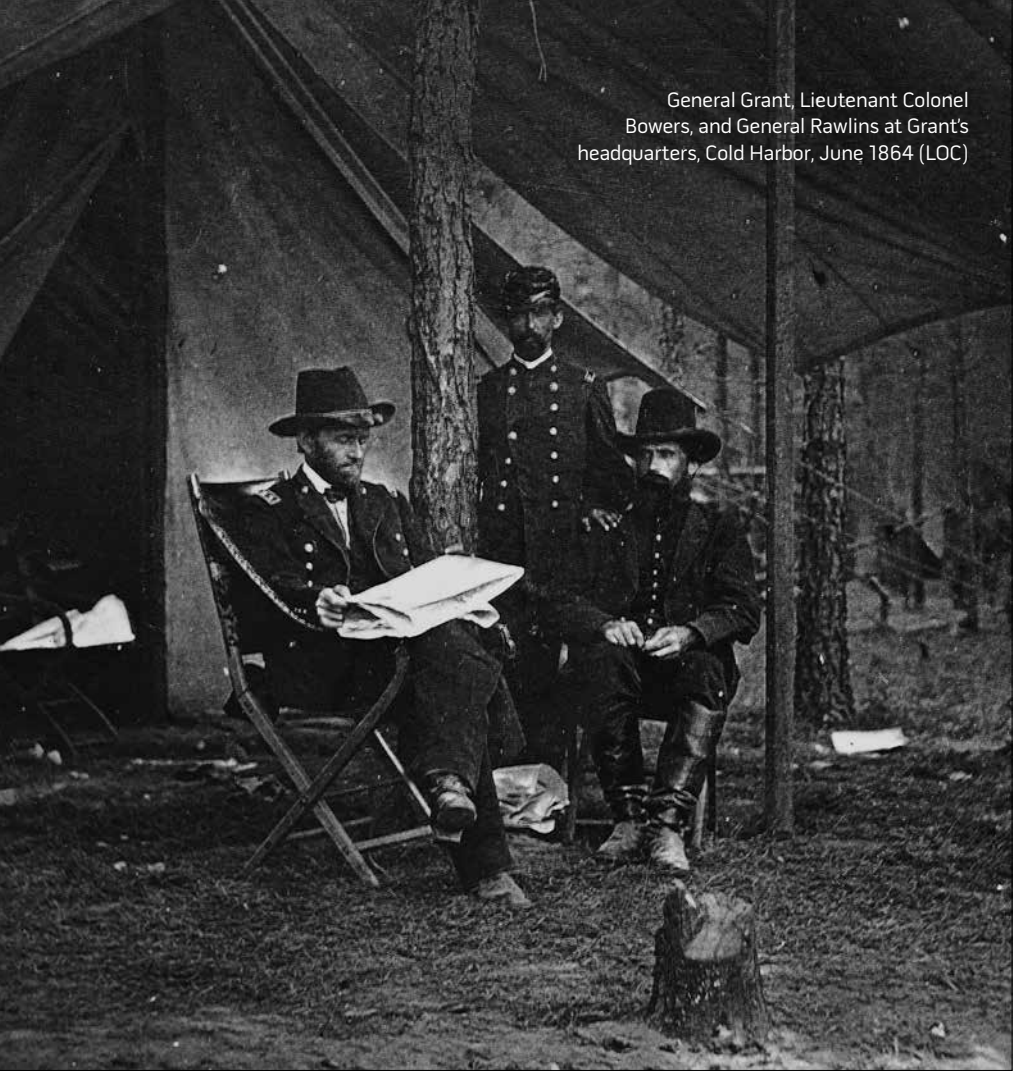
[25] Modinger and Bartlett, 14.

[26] Ibid., 37.

[27] *Remaking Bagram: The Creation of an Afghan Internment Regime and the Divide Over U.S. Detention Power*, Regional Policy Initiative (Washington, DC: Open Society Foundations, September 6, 2012), 7, available at <www.opensocietyfoundations.org/sites/default/files/BagramReportEnglish.pdf>.

[28] See Defense Institute of International Legal Studies, available at <https://www.diils.org/organization/defense-institute-international-legal-studies>.

[29] Fyodor Dostoevsky, *The House of the Dead or Prison Life in Siberia* (Boston: E.P. Dutton & Company, 1914), 130.



General Grant, Lieutenant Colonel Bowers, and General Rawlins at Grant's headquarters, Cold Harbor, June 1864 (LOC)

Union Success in the Civil War and Lessons for Strategic Leaders

By John Erath

On April 10, 1865, Robert E. Lee wrote a letter to the soldiers of his army that began, "After four years of arduous service, marked by unsurpassed courage and fortitude, the Army of Northern Virginia has been forced to yield to overwhelming numbers and resources."[1] At this moment, the Civil War essentially ended in victory for the Union, and the process of reuniting the United States of America began. Lee's immediate view of the circumstances, that the Confederate armies had done everything possible but were overmatched by Northern numbers, provided a means by which his veterans could feel that they had served honorably, but it was challenged almost immediately by other Confederate military and political leaders who blamed instead such factors as incompetent government, social divisions, and political squabbling for their defeat. The Confederacy, many felt, would not have embarked on a war it could not win.[2] Indeed, its success in repelling invasions over the first 2 years of the war led many to believe that the war had almost been won.

A century and a half later, there remains considerable debate among historians as to the reasons for the outcome of the Civil War. Many explanations have been proposed for the Union victory: political, economic, military, social, even diplomatic.[3] Strong cases can be made as to why each was important to the Confederacy's downfall. Yet the key to victory was found in 1864, after President Abraham Lincoln appointed General Ulysses S. Grant the commander of all Union forces. In concert with Lincoln's other strategic efforts to weaken the Confederate will to resist, Grant devised a military plan that ultimately gave Lee no choice but to surrender. Although there was no written plan, Lincoln and Grant combined the separate elements of Union power in a complementary way to make continuing the war more painful to the Confederate population than rejoining the Union. This comprehensive strategy, which included political, economic, and diplomatic elements as well as military operations, led to victory.

By the early 20th century, however, a consensus had emerged among many Americans that endorsed General Lee's view of how the war ended: the Union simply had advantages in population and economy that made victory inevitable. The United States has enjoyed such advantages in every subsequent conflict and has generally sought to take advantage of them. Yet Lee's perspective

John Erath is a 2014 graduate of the National War College. He is a Foreign Service Officer, currently serving as Senior Advisor to the Bureau of International Security and Nonproliferation at the Department of State.

was simplistic. When American leaders have been successful in war, it has been because they, as did Grant and Lincoln in 1864, implemented an overarching strategy that incorporated all aspects of U.S. power to achieve results; brute force and abundant resources alone are most often insufficient to achieve the desired outcome. By orchestrating a complete national strategy, Lincoln and his top general, Grant, provided the template for American success in war—a template that 21st-century strategic leaders would be well advised to follow.

Grant Changes the Game

In February 1864, Lincoln appointed Grant General-in-Chief of the Union armies, and they began piecing together the means to win the war. For over 2 years, Lincoln and his commanders pursued objectives without a unifying strategic goal. The only experience of strategy for most Americans was the war with Mexico (1846–1848) against a dictatorship in which the strategy was straightforward: defeat the army and capture the capital. More comprehensive means were needed against a large democratic opponent. Despite a string of Union successes in mid-1863, including Gettysburg, Vicksburg, and the capture of Chattanooga, Union prospects remained uncertain, and the new year would include elections in which voters unsatisfied with the progress of the war could support an accommodationist government. In the east, Army of the Potomac Commander General George Meade had not followed up the defeat of the Confederate invasion of the North with significant offensive operations, and Lee's army remained a potent force. In Tennessee, Union forces had advanced about 70 miles in the previous year but suffered a major reverse at Chickamauga. In the West, an epic blunder had allowed Grant to capture a small Confederate field army at Vicksburg and open the Mississippi River to commerce, but Confederate cavalry raids threatened supply lines and kept Union forces from straying far from rivers, thereby preventing the occupation of much territory. In short, over 2 years of bloody war had resulted in the liberation of exactly one state (Tennessee) and some small areas near waterways.[4] It must have seemed to many in the North that subduing the entire Confederacy would be a task beyond the scope of Union resources. On February 3, 1864, the *New York Times* wrote that more men would not be enough to win the war and could never occupy all Southern territory.[5]

There were three main reasons for the Union's slow progress in the war up to 1864. First was the superiority of the defense in 19th-century warfare. A generation earlier, Prussian military theorist Carl von Clausewitz, reflecting upon his experiences in the Napoleonic Wars, had called defense "the stronger form of waging war."[6] The introduction of the rifled musket in the 1850s amplified the advantage of the defense by more than tripling the effective range of infantry. When coupled with improved methods of field fortification, Civil War–era armies were almost invulnerable to frontal assault, as the Union learned at Fredericksburg and the Confederacy at Gettysburg. Even if one side could manage an attack on an unprotected flank, armies had a degree of tactical flexibility that allowed withdrawals in good order to strong defensive positions. Lee's tactical masterpiece at Chancellorsville forced a Union retreat across the Rappahannock and Rapidan rivers but did not destroy the Union army; in fact, Lee suffered proportionately much higher losses in victory.[7]

The Confederacy also possessed the advantage of being able to concentrate forces in response to Union offensives. In addition to operating on interior lines, Confederate armies were able to make use of railroads to move forces to locations threatened by Union operations. The Confederates used their strategic mobility to its best effect during the Chickamauga campaign, when they came closest to destroying a Union army after achieving local superiority through strategic movements of troops. Any effective Union strategy for 1864, therefore, would have to address the potential for such concentrations.[8]

Finally, the Union effort was hamstrung by logistical difficulties. Civil War armies required huge amounts of food, fodder, ammunition, and other equipment. Large land areas and poor roads, especially in the West, meant that armies were confined to operating near rivers and railroads. Even railroads were highly vulnerable to raids from cavalry and irregular forces. Grant's first effort to approach Vicksburg had been defeated almost bloodlessly by Confederate cavalry raids. When he later operated successfully against the city, almost half of Grant's overall forces remained in Memphis and western Tennessee to protect his supply lines.[9]

Given these constraints, it would seem that Civil War armies would have had the most success by avoiding battles, except on unusually favorable terms and using the strategic mobility afforded by railroads to interdict enemy logistics. While commanders, particularly the Confederates in the West, sometimes used this approach, both armies, as well as their civilian leaders, still looked at battle as a path to victory.[10] Civil War commanders therefore faced almost continual pressure, from Bull Run until the end of the war, to seek battle as a means to destroy opposing armies, despite mounting evidence of the near impossibility of a Napoleonic battle of annihilation. Lee thoroughly outmaneuvered Joseph Hooker at Chancellorsville, but he made no further progress once the Union army established a firm defensive position. At Stones River in late 1862, both armies outflanked each other but ended up pounding on their opponents' positions for little gain. In both the North and South, public attitudes on the progress of the war were disproportionately shaped by the results of battles, especially those in the eastern theater. General Ambrose Burnside's disastrous attack at Fredericksburg was in part motivated by political pressure to take the offensive against Lee. In 1864, Confederate President Jefferson Davis removed Joseph E. Johnston from command of the Army of Tennessee and appointed John Bell Hood to force attacks on William T. Sherman's army, an action that hastened

the fall of Atlanta and may have helped Lincoln's reelection. On the eve of the war's most complete battlefield victory, Nashville, Grant went so far as to order the relief of his field commander, General George Thomas, for being slow to attack. Fortunately, the order did not arrive until after Thomas's Army of the Cumberland had routed its opponent.[11]

The task that faced Lincoln and Grant in early 1864 was formidable. Both understood that the Union would not be able to occupy all of the South in the face of armed resistance—the aim of earlier Union strategy—or to destroy its armies by attacking them in the field. A purely logistical strategy, similar to that proposed by General-in-Chief Winfield Scott's much-derided "Anaconda Plan," would be difficult in an agriculturally self-sufficient area, and the South's rapidly developing war industries gave it the capacity to resist potentially indefinitely. By 1863, initial shortages of war materiel, especially weapons and ammunition, were largely a thing of the past; the army Lee took north in June was roughly proportionate to its opponent in numbers and quality of artillery, and almost all of its infantry had modern rifles.[12] The Union did, however, possess several advantages that could be brought to bear. Abraham Lincoln had proved an outstanding wartime political leader and by 1864 had in place a strong leadership team, including Secretary of War Edwin Stanton, Secretary of State William Seward, Army Chief of Staff Henry W. Halleck, and Quartermaster General Montgomery Meigs. The Union Army benefited from outstanding management and supply as a result. Lincoln's political skill had maintained consistent support for the war effort in Congress and patience among the Northern public when faced with military reverses. The Emancipation Proclamation was a decisive political stroke that had associated Union war aims with moral objectives. The Union also had, after much trial and error, placed most of its military forces in the hands of skilled leaders who had come to understand 19th-century war and were at least equal to their Confederate counterparts.

Grant's goal was to find ways to use these advantages to overcome the factors that had previously thwarted Union efforts. Without an overarching strategic focus, the Union directed its actions at targets of opportunity—armies or geographic features—for short-term objectives rather than to win the war. Prior to 1864, the political process too often drove military decisions, leading to ill-advised attacks, such as those at Bull Run and Fredericksburg. Union generals did not receive clear strategic guidance and often had to pursue multiple objectives, including trying to destroy Confederate armies, occupying territory, building railroads, and protecting supply lines. After the fall of Vicksburg in July 1863, Grant's army spent most of the summer relatively inactive, except for some local raiding, without an immediate strategic objective.

Piecing the Elements of Strategy Together

It is difficult to evaluate the 1864 Union strategy because it never appeared as a single document, nor was it articulated as a whole in Grant's memoirs or those of other Union leaders. Instead, it must be pieced together from what those involved in its creation have written. Grant's memoirs focus on the military operations that he controlled. At the same time, the Republican political leadership shaped a plan to win reelection while the State Department sought to increase the Confederacy's isolation. As President, Lincoln had to coordinate these efforts as elements of a complete strategy that complemented Grant's military efforts. Grant had likely not been exposed to Clausewitz, but the Prussian theorist would have recognized in Grant's strategy the targeting of the enemy's center of gravity the key to his resistance. Based on his analysis of the Napoleonic Wars, Clausewitz believed the center of gravity generally to be the army, although sometimes it was the national leadership and the nation's capital city. The Civil War was the first conflict since ancient times between two democracies (or perhaps two versions of one democracy).[13] As such, the center of gravity had to be different from those found in European monarchies. Grant and Lincoln intuitively grasped that the only way to win the war was to break the support of the Southern population for continuing its war effort. In Clausewitzian terms, the Union identified public support for the war as the Confederate center of gravity, providing a formula for those seeking to defeat democracies to this day. The Confederates, to some extent, figured out this formula before the Union did. One of Lee's motivations for the second invasion of the North in 1863 was to seek a victory on Northern soil in hopes of inducing the Northern public to believe that the war was unwinnable.

Grant's focus in the broad Union strategic construct was the military effort aimed at the Confederate armies and their sources of support. Grant and his top subordinate, General Sherman, formed their operational plans based on previous experiences, including trying to avoid frontal attacks such as Fredericksburg or Sherman's unsuccessful assault on the Chickasaw Bluffs near Vicksburg. The defeat at Chickamauga led to heightened concerns that the Confederates would again move troops from one army to another to gain local superiority. Grant wrote that his plan was for Union forces to concentrate against the two main Confederate field armies. He ordered Sherman, commanding in the West, to "move against [Joseph E.] Johnston's army and break it up," while telling Meade in Virginia that Lee's army was his objective. Grant also included smaller forces, in Tennessee, West Virginia, and tidewater Virginia, in his plan by directing them against key production and transportation facilities that supported armies in the field. Once Sherman captured Atlanta, the bulk of his forces became in effect a large raiding party aimed at damaging Confederate means of supply. Historian Archer Jones refers to the Union concept as a "raiding logistics strategy," in which opposing armies would be deprived of the means to continue operating, and attributes Union victory to its implementation.[14] While the Union's increased focus on

Confederate sources of supply played a role in the Confederate defeat, it was not alone decisive. To the end of the war, Confederate armies maintained the ability to resist, and although they suffered shortages, they managed to obtain what they needed to keep fighting.

While Grant was planning his 1864 campaigns, Lincoln took political measures to promote Union success. With Lincoln's Democratic opponents planning to run on a peace platform, reelection was vital to overall Union prospects, but a steady stream of indifferent military news made a Lincoln victory seem unlikely until weeks before the election. The political and military policies were therefore dependent on each other: to win the war, the Union needed Lincoln's reelection, but to win in November, Lincoln required military success. The war's most important policy step, the Emancipation Proclamation, had been issued a year earlier and had the effect of solidifying the moral basis for the war as well as opening the door to the recruitment of significant numbers of black troops. Lincoln's 1864 publication of the relatively mild terms under which Southern states would be readmitted into the Union (which, as with the Emancipation Proclamation, Lincoln did without congressional authorization), while initially greeted with scorn, served to provoke debate in the Confederacy as to whether further resistance would be worse than submission.[15]

The Union's economic policy likewise had the effect of making life more difficult in the South. By 1864, the majority of Confederate ports were in Union hands, but even in 1864, 84 percent of ships attempting to run the blockade succeeded. In any event, against an agricultural society such as the Confederacy, a blockade was unlikely to produce much real hardship. Although the South initially lacked war materiel, by 1862 it developed production facilities adequate to supply its forces with arms and ammunition, so as not to depend on imports.[16] (When the U.S. Army opened its new Infantry Museum in Fort Benning, Georgia, in 2009, it "guarded" the entry to the main exhibits with 2 12-pounder cannon produced by Georgian foundries during the war.) The blockade did have two important effects. First, it restricted the supply of luxury goods being imported, creating an impression of hardship, especially for the ruling class. It also deprived the Confederate government of customs revenues, the primary source of government income in the 19th century. The most severe economic blow to the Confederacy was self-inflicted. By cutting itself off from the financial system of banks, the South deprived itself of necessary capital and, by financing its military with unsecured paper money, started itself down the road of hyperinflation.[17]

Members of Grant's staff during main eastern theater of war, siege of Petersburg, Virginia, June 1864–April 1865, with photographer Mathew Brady standing at far left (LOC)

Other aspects of U.S. policy also contributed to achieving the conditions for victory. From the beginning of hostilities, Union diplomatic efforts aimed at preventing foreign recognition of the Confederacy. Secretary of State William Seward instructed U.S. diplomatic missions to inform foreign governments that the conflict was not legally a war, but an internal dispute, in effect declaring that any recognition of the Confederacy would be contrary to international law. Seward was concerned because European governments, particularly the United Kingdom, viewed the United States with suspicion. The American minister in St. Petersburg, Cassius Clay, gave Seward his view of the sentiment in Europe in 1861: "They hoped for our ruin. They are jealous of our power."[18] The Emancipation Proclamation proved the key diplomatic stroke of the war as it equated support to the Confederacy with support for slavery, an unacceptable stance in most of Europe. While there may have been some sympathy for the Southern cause, or at least desire to see the Union broken, the political cost of support to the South had become too high. Confederate leadership had begun the war with high expectations of European support. When it did not

materialize, the South's sense of isolation increased.

The Union's final strategic advantage was in how its policies contributed to maintaining popular support while eroding it in the South. The Lincoln administration by 1864 had developed methods of dealing with the press to obtain favorable coverage from many of the major East Coast newspapers. When the Army of the Potomac was locked in a bloody stalemate at Spotsylvania in May 1864, the *New York Times* reported, "The terrible pounding the rebels received . . . has compelled them to fall back. . . . Lee's retreat [is] becoming a rout."[19] The appointment of Grant to overall command was as much a public relations move as a military one and was intended to show the Northern public that the Union now had military leaders comparable to those of the South. Grant, in fact, was under a great deal of pressure to take personal charge of the Virginia theater to confront Lee directly. Because, unlike previous Union commanders, Grant did not seek to win the war through a decisive battle, he did not undertake the sort of risky operations that had led such commanders as John Pope, Ambrose Burnside, and Joseph Hooker to defeat. Conversely, the fact that Lee could not clearly win a battle against Grant had a significantly negative effect on Southern morale.[20]

Turning the Tide

Even though the Union employed the elements of a comprehensive strategy in 1864, victory still proved difficult. The simultaneous offensives of the main armies succeeded in preventing Confederate concentrations but did not result in the battlefield victories the public was expecting. In the east, Grant and Meade faced Lee in a relatively small theater where scant room for maneuver meant the armies remained in nearly constant contact, building huge casualty lists for little tactical advantage. In the West, Sherman's army avoided frontal attacks by using the larger area of operations to outflank Confederate positions. Although he advanced against Atlanta, the Northern public again expected successful battles.[21] Incompetent political appointee generals stymied Grant's plans to disrupt Confederate logistics with raids in the Shenandoah and up the James River toward Richmond.[22] In the summer, there was considerable doubt that Lincoln could be reelected; John C. Fremont even mounted a challenge for the Republican nomination. The Democrats approved a peace platform, in effect declaring the war unwinnable.

Meanwhile, the war was being won. After spending May and June repeatedly trying to move around Lee's right flanks only to encounter entrenched Confederate defenses, Grant managed to surprise Lee by bypassing Richmond, crossing the James, and moving on Petersburg. The capture of this city would cut most of the supply lines to Richmond and Lee's army and potentially force Lee to attack at a disadvantage. Only dawdling by subordinate commanders kept the Union from seizing Petersburg, but Grant still pinned the Army of Northern Virginia in a siege. Neither side wanted this situation. Lee believed that it would be "only a matter of time" before he would be forced to give up his capital.[23] The Union leadership, mindful of the siege of Sevastopol in the Crimean War, where allied armies suffered crippling losses taking the city, was concerned that the Army of the Potomac would waste away in the trenches while their opponents remained secure in the city.[24] By trapping Lee's army, however, Grant could dispatch General Philip Sheridan to the Shenandoah, a critical source of supply for the Confederate army. Sheridan won three battles against smaller Confederate forces, giving the Union needed battlefield successes.

At the same time, Sherman approached Atlanta. His Confederate opponent, Joseph E. Johnston, had adopted the same approach the Russians had in 1812, trading territory for time and lengthening the enemy's supply line. By the time Sherman neared Atlanta, almost 30 percent of his original strength had diminished from attrition and the need to protect his line of communications.[25] Confederate political leaders had grown impatient with the apparent lack of decisive action, and Jefferson Davis replaced Johnston with John Bell Hood, who had lobbied for the job with promises he would seek immediate battle. Hood attacked three times, and the defensive advantages of Union armies led to three defeats. When Sherman cut Atlanta's last railroad on August 31, Hood evacuated the city.

Atlanta was an important industrial and transportation hub; its loss, however, had greater significance. The Confederacy still had other operational railroads and could make up much of Atlanta's production elsewhere, but the city's fall provided a highly visible sign that the Union was making progress in the war. This apparent progress came at an ideal time in the political season. Together with a continuing economic expansion, military success provided an electoral college landslide. While Lincoln might have won the election without Sherman's success, it effectively undercut the main argument of Democratic candidate George McClellan: that Lincoln was doing a poor job running the war. With preventing Lincoln's reelection a key strategic goal of the Confederate government, the election result signified that continuing the fight meant 4 more years of an increasingly terrible war. In South Carolina, Mary Chesnut, the wife of one of Jefferson Davis's advisors, wrote, "Atlanta gone . . . No hope. We will try to have no fear. . . . We are going to be wiped off the face of the earth."[26]

Following Atlanta's fall, Sherman shifted his operational stance from an offensive against a Confederate army and its base to one of raiding the Confederate heartland without conquering territory. Jefferson Davis approved Hood's plan to attack Sherman's line of communications back to Tennessee, not understanding that as a raiding force, Sherman's army could operate independently of its supply source. Grant ordered forces detailed to protect Tennessee to concentrate at Nashville under the command of General George Thomas, probably the war's best field commander, to deal with Hood. This move allowed Sherman's force to become what Grant termed a "spare

army." Its target was not Confederate soldiers, but rather the Southern will to fight. As Sherman put it, "This movement is not purely military or strategic, but will illustrate the vulnerability of the South . . . and make its inhabitants feel that war and individual ruin are synonymous."[27]

By the end of 1864, the situation in the Confederacy had changed dramatically. Its armies had been unable to win on the battlefields. The Davis administration appeared increasingly ineffectual. Union armies neutralized centers of production and transportation, leading to shortages for the armies and on the homefront. Union armies seemed to march where they wished without serious opposition, striking at the idea that the Confederate government could perform the most basic of functions: control its own territory. With Lincoln's reelection, the chance that the North would tire of the war seemed increasingly slight.

At the same time, a political division emerged in the South. At the war's outset, most of the Confederate leadership would have agreed with Jefferson Davis's statement that the South had gone to war to preserve slavery. By 1864, with the Emancipation Proclamation issued, much of the Southern population saw the issue differently. Many Southerners had come to consider self-determination and independence more important war aims.[28] There had always been a contradiction for the majority of Confederate soldiers who did not own slaves but were fighting for a slave-owning elite's right to maintain their "institution." The issue was highlighted on January 2, 1864, when General Patrick Cleburne proposed offering freedom to slaves who enlisted in the Confederate army. Cleburne's proposal was quickly shelved by his superiors, but the debate as to whether the South was fighting for independence or slavery grew, sapping enthusiasm for continuing the war. To fight the war effectively, the Davis administration had taken centralized authority over war-related industries and railroads. By doing so, however, it alienated the large segment of its population that believed that the war was about states' rights and freedom from central government control. To maintain a strong military, the Confederate government undermined its own base of support.[29]

As 1864 ended, the Union clearly held the upper hand militarily. The December 15–16 Battle of Nashville, where the Union achieved the victory of annihilation that both sides sought early in the war, erased any doubts about Northern prospects. For only the second time in the war, an entrenched army was successfully attacked and routed from the field by General Thomas's careful planning and tactical misdirection. The Confederate Army of Tennessee ceased to exist as a threat to Union armies (although some of its units were cobbled together under Joseph Johnston to harass Sherman in the Carolinas), leaving Lee's besieged force as the Confederacy's last effective field army. Even though Union armies had gained little territory in 1864, Lincoln's strategy had decided the outcome. In January 1865, Mary Chesnut wrote, "The end had come. The means of resistance could not be found."[30]

The end came quickly once the spring weather allowed campaigning in Virginia. Although Lee's army remained intact, it was worn down by supply shortages, desertions (especially by troops from regions threatened by Sherman's raids), and political alienation. Grant moved a portion of his army west of Petersburg, cutting its rail connections and threatening to isolate the Army of Northern Virginia from its sources of supply to the south and west. Lee would not be caught in such a trap and maneuvered to escape west. Plagued by supply problems, he was finally stopped by Union forces at Appomattox Court House. Faced with having to attack a prepared Union position, Lee decided to avoid further bloodshed and surrendered on April 9. A week later, Johnston surrendered the other Confederate forces to Sherman. Although there were still thousands of Confederates under arms who could have resisted almost indefinitely as guerrillas, the will to fight on was gone, and the war ended.[31]

While it would have been possible for Confederate forces to continue fighting, hostilities ceased except for some isolated groups. Armies were still in the field, but the marginal cost of war was far beyond any possible benefit. Lincoln's liberal terms for readmission of the Southern states into the Union, initially maintained by Andrew Johnson after Lincoln's assassination, also facilitated the transition to peace. Lincoln's economic policies had contributed to the Union victory by creating shortages that squeezed the South's ruling class, but his Reconstruction plan did not include measures to build the economy beyond unsuccessful efforts to provide agricultural opportunities to former slaves. Lincoln's second inaugural address summarized his approach to putting the country back together: "With malice toward none, with charity for all, with firmness in the right as God gives us to see the right, let us strive on to finish the work we are in, to bind up the nation's wounds, to care for him who shall have borne the battle and for his widow and his orphan, to do all which may achieve and cherish a just and lasting peace among ourselves and with all nations." Whatever the shortcomings of Reconstruction, Lincoln's policy created the political space to solidify peace.

The Union had victory, forcing the Confederacy to abandon all its war aims. It accomplished this goal despite the South holding the advantage of strategic defense, having parity of military leadership, and needing not total victory, but merely to maintain resistance until the other side tired. In 1958, with the war's centennial approaching, Gettysburg College sponsored a conference on why the North won. The findings were later published as a series of essays, each of which examined one factor: political, military, economic, and diplomatic. While the authors noted that there was no one explanation and that advantages in each of these categories contributed to victory, none of the contributors took the next step to consider these elements as essential parts of an overall strategy that won the war.[32] Without any one component, the result might have been different. In 1862, for example, the Union tried to employ superior numbers and economic strength, but such commanders as

Ruins of Richmond, Virginia, 1865 (NARA/Mathew Brady)

General George McClellan squandered its advantages. McClellan continually demanded more troops of Lincoln, without solid plans for how they would be employed to achieve his goals of defeating Lee's army and capturing Richmond. His assumption was that reaching these goals would be sufficient to end the war, but the South in 1862 survived battlefield losses and still had plenty of will to fight on.

Clausewitz as Civil War Strategist

If war, as Clausewitz famously wrote, is policy by other means, then successful war requires a clear policy objective combined with the means to achieve it. By eventually coordinating military operations with political, economic, diplomatic, and other efforts, the Union leadership was able to develop a set of policies that gave it a decisive strategic advantage. The Union strategy addressed all three of Clausewitz's "trinity" of bases for a state to maintain a war effort—the army, government, and people—while wrecking the Confederacy's passion, creativity, and reason—the Prussian theorist's "first trinity" of motivations for a people at war. After inflicting losses on Confederate armies, demonstrating the government's inability to control its territory and increasing the costs of continued resistance to the Southern people, Lincoln created the conditions for victory.

The Confederacy did not arrive at a comprehensive strategy. Davis and Lee correctly identified a strategic goal: eroding Union morale so that Lincoln would lose the election. The Southern leadership did not, however, support this goal with the necessary means to achieve its end. The Confederacy depended almost exclusively on its field armies winning battles to prove the war unwinnable for the North. Lee, in particular, proved effective on the tactical and operational levels, and the Davis administration managed to provide the materiel to keep its forces in the field. These successes, however, were not matched in the political and economic dimensions. The effects of this shortcoming were felt increasingly as the war continued; economic hardship and increasing disunity over the future of slavery took their toll on the South's will to continue.

Almost as soon as the war ended, analysis of it began. Many in the South tried to pinpoint why they had lost a war they believed had been winnable. In the North, it was easy to attribute victory to the moral superiority of the Union. For ex-Confederates, things were more complicated. The South had fought hard for 4 years, and many had come to dismiss slavery as the reason for the long struggle, focusing instead on self-defense.[33] While many agreed with Lee's assertion that numbers and resources weighed against the South, others looked elsewhere for explanations. Confederate General Pierre G.T. Beauregard wrote that "no people ever warred for independence with more relative advantages."[34] Others, such as Joseph Johnston and James Longstreet, pointed to supposed inadequacies of Davis's political leadership or that of state governments that put local needs above those of the Confederacy.

By the end of the 19th century, however, most accounts of the war had moved toward the population-resources theory, what historian Richard Current referred to as "God and the heaviest battalions."[35] A 1908 textbook explained that "the North must finally win, if the struggle went on, for its resources were varied and practically unlimited."[36] During the postwar era, the most important national objective was to reconcile the two sections of the country after 4 years of destruction. With reunification taking priority over social justice, the elements of segregation and institutionalized racism developed as long as secession remained off the table.[37] Similarly, the idea that the Confederacy had fought the good fight in its own defense and was overwhelmed despite superior military leaders became part of the standard narrative of American history. A textbook published in 1916 reduced the war to a summary of battles and generals, with no mention of overall strategy.[38] In the 20th century, historians produced shelves full of books on the Civil War, with most taking a more nuanced look at its outcome. British military theorist B.H. Liddell Hart blamed Lee's aggressive tactics for eroding Confederate military strength and lauded Sherman's "indirect approach."[39] Others, such as Frank Owsley in 1925, blamed the doctrine of states rights for undermining Confederate unity.[40] None of this work, however, was able

to shake the hold of the "overwhelming resources" explanation. In January 2014, in an Internet search of "Why did the Union win the Civil War," over 90 percent of the hits were some variation of the inevitability of Northern victory by superior numbers.[41]

Lessons Learned

Since the Civil War, the United States has employed a variety of strategies in military conflicts, but in all of them has sought to apply advantages of size and productive capacity. In World War I, the overall strategy of attrition was set by Allies, and the U.S. contribution was generally perceived as supplying military mass. Recent scholarship, however, has taken a more positive view of U.S. performance in the 1918 offensives.[42] It was the presence of large U.S. forces on the battlefield that provided political weight to Woodrow Wilson at the peace negotiations, influence he chose to use to push for a League of Nations rather than an equitable settlement in Western Europe.[43] U.S. strategy during World War II again combined diplomatic, political, and economic elements with military operations. U.S. assistance, for example, was important to keeping the Soviet Union in the war and maintaining the strength of the Alliance while U.S. forces built up for the invasion of Europe. U.S. Navy submarine operations played a key role in degrading the Japanese economy by cutting off its supplies of raw materials. Much as with the Civil War, however, many popular accounts of the war focused on industrial production as a deciding factor. NBC television's influential documentary *Victory at Sea* devoted most of an episode to the way the United States was able to pour resources into the fight. Similarly, the country succeeded in the Cold War by implementing a comprehensive strategy of containment, first articulated by George Kennan in 1947, which employed all elements of state power to promote "either the break-up or gradual mellowing of Soviet power."[44] In 2011, however, *New York Times* writer Leslie Gelb assigned credit for the Cold War's conclusion to the strength and productivity of the U.S. economy.

Men repairing single-track railroad near Murfreesboro, Tennessee, after Battle of Stone's River (LOC)

In Vietnam, the United States faced a situation in which its ally, the South Vietnamese government, could not function effectively. As the war went on, the United States came to rely increasingly on massive firepower to achieve success on the battlefield without accompanying political and economic elements. While the primary reasons for the overreliance on military power were undoubtedly domestic political concerns, by the 1960s, Americans had become accustomed to the idea that superior numbers and resources could win wars. Vietnam prompted many reviews of such assumptions, so that in the 1991 war against Iraq, the George H.W. Bush administration combined its huge advantage in military technology with a diplomatic campaign to build a coalition, economic sanctions, and effective public messaging to ensure success. In 2003, the use of superior force was repeated, but without a suitable strategy to transition from military success to a sustainable peace.

More recently, the importance of strategy has been reinforced. President George W. Bush intended the 2007 "surge" in U.S. troops in Iraq to provide security and allow time for political development. The White House coordinated its plan with Iraqi government policies and the political and economic strategy of the U.S. Embassy. The administration of Barack Obama then attempted to duplicate the strategy's apparent success with a surge of its own in Afghanistan in 2010. Press coverage of the decision-making process in 2010 focused almost exclusively on the issue of troop numbers and whether U.S. Commander General Stanley McChrystal would receive the reinforcement he demanded—a situation reminiscent of General George McClellan's demands of Lincoln in 1862.[45] As of early 2014, despite some success against the Taliban, the overall violence remains unabated, and the Afghan

government still shows little evidence of providing for its own security. This development leads to the question: did the surge become an end in itself rather than an instrument of a broader strategy?

Strategy matters. By matching military objectives to political, diplomatic, and economic policies, Lincoln and Grant were able to overcome the Confederate defensive advantages that had stymied the Union for over 2 years. While the Lincoln administration never put together a strategy document like the 21st-century National Security Council does, all of the elements that would go into a modern strategy were present. By combining the policies of the civilian government with military operations, the Union affected the true center of gravity of the Confederacy: the will of its people to resist. Just as the post–Goldwater-Nichols U.S. military used joint forces to increase military effectiveness, the coordination of policies provided a significant force multiplier. From the Mexican War on, advantages in population, resources, and production have been among the most important tools for American success in conflicts. The United States has experienced problems when it relies too much on this set of tools without employing them in the context of a comprehensive policy, and the example of the Civil War can apply to policymakers of the 21st century. Abraham Lincoln stated, "Human nature will not change. In any future great national trial, compared with the men of this, we shall have as weak and as strong, as silly and as wise, as bad and as good. Let us therefore study the incidents in this as philosophy to learn wisdom from." From the Union victory, Lincoln might have advised posterity of the vital importance of being strategic. JFQ

Notes

[1] Robert E. Lee, "Farewell Letter to the Army of Northern Virginia," in *Battles and Leaders of the Civil War*, vol. IV, ed. Robert Johnson and Clarence Buel (New York: Thomas Yoseloff, 1956), 747.

[2] Richard E. Beringer et al., *Why the South Lost the Civil War*, reprint ed. (Athens: University of Georgia Press, 1991), 424.

[3] For extensive discussions of each of these factors, see David Herbert Donald, ed., *Why the North Won the Civil War* (New York: MacMillan Publishing, 1960), for a collection of essays highlighting the various arguments.

[4] Herman Hattaway and Archer Jones, *How the North Won: A Military History of the Civil War* (Urbana: University of Illinois Press, 1991), 490–491.

[5] "The Future Military Policy," *New York Times*, February 3, 1864.

[6] Carl von Clausewitz, *On War*, ed. and trans. Peter Paret and Michael Howard (Princeton: Princeton University Press, 1989), 358.

[7] Archer Jones, *Civil War Command and Strategy: The Process of Victory and Defeat* (New York: Free Press, 1992), 158.

[8] Donald Stoker, *The Grand Design: Strategy and the U.S. Civil War* (Cary, NC: Oxford University Press, 2012), 352.

[9] Hattaway and Jones, 312.

[10] Jones, 235.

[11] Benson Bobrick, *Master of War: The Life of General George H. Thomas* (New York: Simon & Schuster, 2009), 289.

[12] Beringer et al., 215.

[13] It can be argued that the American Revolution and War of 1812 were fought between democratic opponents, but democracy at the time, particularly in Britain, was rudimentary. The British system of the time was a still-developing constitutional monarchy. Had it been truly democratic, the British public likely would have tired of the war long before King George and the Tory government.

[14] Jones, 184.

[15] Beringer et al., 307.

[16] Ibid., 201.

[17] Ibid., 11.

[18] Donald, 57.

[19] Harold Holzer and Craig Symonds, eds., *The New York Times the Complete Civil War 1861–1865* (New York: Black Dog & Leventhal Publishers, 2010), 334–335.

[20] Hattaway and Jones, 571.

[21] Ibid., 570.

[22] Ibid., 558.

[23] Bruce Catton, *This Hallowed Ground* (New York: Pocket Books, 1961), 405.

[24] Hattaway and Jones, 593.

[25] "Atlanta Campaign," *The New Georgia Encyclopedia*, available at <www.georgiaencyclopedia.org/articles/history-archaeology/atlanta-campaign>.

[26] Mary Chesnut, *Mary Chesnut's Civil War*, ed. C. Vann Woodward (New Haven: Yale University Press, 1981), 642, 645.

[27] Hattaway and Jones, 640.

[28] Beringer et al., 380.

[29] Ibid., 425.

[30] Chesnut, 704.

[31] Beringer et al., 345, 403.

[32] Donald.

[33] See Beringer et al., chapters 15 and 17. The authors argue that the shift in Southern thinking began during the war as a way to keep its forces motivated, then was solidified by postwar myth-making, focused on "The Lost Cause." With a consensus emerging that slavery had been morally wrong, Southern apologists chose to focus on self-defense as the reason for their resistance.

[34] For a commentary on the reason for Southern defeat, see Beringer et al., 425–443. The authors draw a parallel with the performance of Paraguay in the War of the Triple Alliance (1865–1871). The Paraguayans, though facing much greater odds in terms of population, economy, and resources (some Paraguayan units were armed with pikes), were able to resist for a longer period by using the advantages of strategic defense. Their enemies, Brazil, Argentina, and Uruguay, relied largely on their numbers to overwhelm Paraguay.

[35] Donald, 32.

[36] Andrew Cunningham McLaughlin, *A History of the American Nation* (New York: D. Appleton and Co., 1908), 467.

[37] Beringer et al., 412.

[38] Samuel Eagle Forman, *First Lessons in American History* (New York: The Century Co., 1916), 286.

[39] Donald, 52.

[40] Beringer et al., 6.

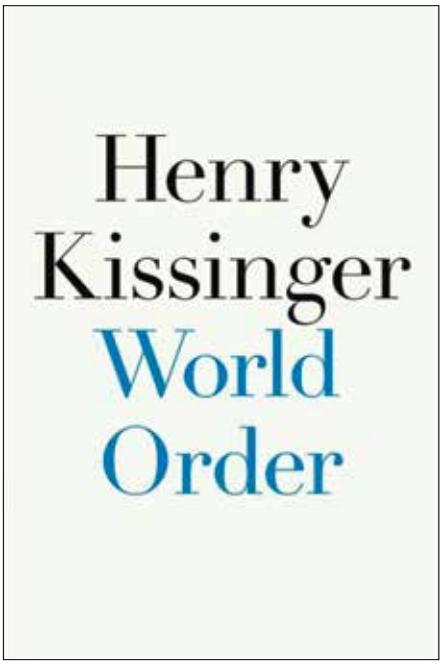
[41] A sample of the common views on the question can be found in "Why the South Lost the Civil War," available at <www.historynet.com/why-the-south-lost-the-civil-war-cover-page-february-99-american-history-feature.htm>.

[42] See, for example, John Mosier, *The Myth of the Great War* (New York: HarperCollins, 2001).

[43] Thomas A. Bailey, *A Diplomatic History of the American People* (Englewood Cliffs, NJ: Prentice Hall, 1980), 605.

[44] John Lewis Gaddis, *George F. Kennan: An American Life* (New York: Penguin Books, 2011), 261.

[45] "The Obama Administration and the War in Afghanistan, 2009–2012," in *For the Common Defense: A Military History of the United States from 1607 to 2012*, ed. Allan R. Millet, Peter Maslowski, and William B. Feis (New York: The Free Press, 2012), 672.



World Order

By Henry Kissinger
Penguin Press, 2014
432 pp. $36
ISBN: 978-1594206146

Reviewed by David A. Anderson

Henry Kissinger, the scholar, statesman, and philosopher, writes a fascinating, insightful, and thought-provoking history of the concept of the state, statecraft, grand strategy, and international cooperation in the pursuit of order and stability among nations. Although no true universal arrangement among states has ever existed, he asserts the order that does exist is at risk because of developing forces beyond the control of states themselves. So we must ask whether collective state order can be achieved while maintaining individual state freedom in an increasingly intricate and turbulent global environment.

The author sets the stage by addressing evolution of the state as a permanent and fundamental entity in conducting international intercourse. He notably highlights the significance of the Peace of Westphalia (1648) in first institutionalizing international order among states. The state became the impetus in establishing foreign policy and the representative strategy for protecting and promoting the best interests of its people, free of foreign intervention based on religion or otherwise. Kissinger smartly details the role of the state in developing European relations and its enduring legacy in shaping the dealings between and among states to this day. Along the way, he draws upon classic philosophers including Immanuel Kant and Thomas Hobbes who have shaped our understanding of the role of the state.

Kissinger painstakingly details the breakdown of international order over time due to imbalances of power and ambitions between and among states. He then examines the collective pursuit by nations to reestablish order through agreements, such as the Congress of Vienna (1814–1815) that spoke to the post-Napoleonic era in Europe. He describes how difficult such agreements became over time owing to varying state historical experiences, perspectives, and interests. As effective as the Congress of Vienna was in bringing stability to Europe, it was no panacea for peace in the long run. Russia in essence ignored it, expanding its borders every year until 1917, while it ultimately provoked a unified Germany into eventual war in 1914. Further exemplifying the difficulty of rebuilding international order resulting from imbalance of power is the disaster known as the Treaty of Versailles, which set the terms for peace at the end of the First World War that eventually led to World War II. Unfortunately, U.S. isolationism ultimately won out over President Woodrow Wilson's League of Nations concept to restore international order. Without U.S. leadership in such an organization, another major war in Europe was inevitable.

In spite of efforts to promote post–World War II international order by establishing organizations such as the United Nations, World Bank, General Agreement on Tariffs and Trade, and International Monetary Fund, a Cold War of differing philosophies supported by military might broke out, pitting U.S. democracy against Soviet communism. The Cold War left both countries vying for the dominant position to dictate and lead international order. Competing multilateral balance of power initiatives such as the North Atlantic Treaty Organization and Warsaw Pact subsequently soon followed. It also set the United States and Soviet Union as opponents in a nuclear arms race, further destabilizing world order.

Kissinger details the trials and tribulations of U.S. strategies during the Cold War period. Although the United States eventually won the war, it has struggled with grand strategy to this day. Examples include the war on terror, Iraq and Afghanistan, Syria, Palestine, an aggressive Russia, nuclear weapons in North Korea and Pakistan, and Iran's pursuit of nuclear weapons. At the same time, China rises as not only an Asian power but also an international one while traditional European allies are in decline. Furthermore, China is by default asked to adhere to principles it did not help shape. As applied, the Chinese are "at odds with its historical image of itself." Finally, Kissinger likens the Iranian revolution that began in 1979 to pre-Westphalia times and commits a significant effort to addressing the disorder in the Middle East (for example, the Arab Spring) and Islamic states in general.

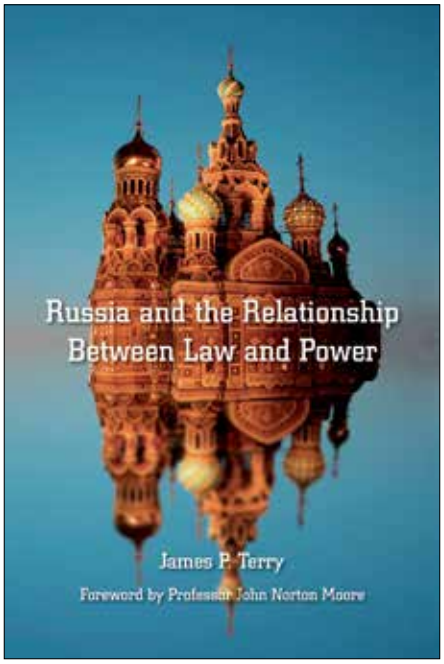
The author underscores the difficult challenge for states to reconstruct international order in today's environment because they inherently pursue self-interests above all else. For that reason, he asserts that no alliance is permanent. Relationships are becoming more intrinsically mixed, notoriously fragile, and frequently wane—depending on prevailing issues. Kissinger ends by leaving the reader to contemplate contemporaneous problems making the revision of the Westphalia model necessary and problematic. Featured topics include the emergence of globalization (placing economic and political institutions increasingly at odds), cyber technology, the human factor in the information/digital age, and nuclear proliferation. He believes international forums such as the United Nations Security Council, the G7, G8, G20, and Asia-Pacific Economic

Cooperation are not conducive, nor comprehensive enough, to tackle the contemporary realities necessitating changes to the international system. This is a challenge for statesmen going forward: revise the world order arrangement or face a fragmented dysfunctional world.

Over the years much has been written regarding the theme of this book. Kissinger's breadth, depth, and astute understanding of the subject matter are beyond reproach and vividly displayed throughout the book. No other author has ever accomplished such a comprehensive feat in such a judicious and finely distinct way. The historical context that only he can provide is evident with a nuanced flavor that is as readable as it is enlightening. It is readily apparent he brings to bear his entire professional experience in writing this fine addition to his seminal body of work.

The book is a must-read by political science, international diplomacy/relations, public administration, and strategic studies students and scholars, as well as government officials, foreign policy designers, and military leaders. It is also relevant to historians and those with a general interest in the history of states and international diplomacy. **JFQ**

Lieutenant Colonel David A. Anderson, USMC (Ret.), DBA, is a Professor of Strategic Studies and the William E. Odom Chair of Joint, Interagency, and Multinational Operations at the U.S. Army Command and General Staff College, Fort Leavenworth, Kansas.



Russia and the Relationship Between Law and Power

By James P. Terry
Carolina Academic Press, 2014
188 pp. $27
ISBN: 978-1611635959

Reviewed by Alice A. Booher

Winston Churchill stated, "Russia is a riddle wrapped in a mystery inside an enigma." James Terry patiently peels away each of those layers to hypothesize an unrelenting consistency and prevailing logic to Russian behavior as it seeks power, for myriad reasons, over those who dwell within and without its self-defined boundaries. The release of this compact yet intricate work by Dr. Terry, addressing the long and convoluted history of Russia and its recurrent international "habits," could not be timelier in multiple contexts.

The timeframe is inclusive of the post-Yalta Soviet Union through 2008, with cogent collateral references to subsequent behaviors. There is a thorough analysis of the Russian vocalized rationalizations versus actions (legal and otherwise) vis-à-vis Afghanistan (which remains in a class by itself), as well as Hungary, Czechoslovakia, Poland, Lithuania, Chechnya, and Georgia. Terry's salient analyses are primarily twofold: first, directed to the Russian forward propulsion of military, economic, political, and cultural decisions through creative interpretation of one or more provisions of already existing legal documents ranging from Geneva Conventions to the United Nations Charter to the Warsaw Pact; and second, in those instances where the reasons proffered for Russian actions were defined in the context of reinvented so-called inherent national interests as the result of its citizens in that territory.

For instance, in discussing the 2008 Russian dealings with the government of Georgia, Terry identifies the prophetically strong message, now heard in its greatest cacophony in Ukraine, that those areas with significant Russian populations "would be viewed as squarely within Moscow's sphere of influence, and be protected." He further observes that the current events in locations such as Ukraine and perhaps elsewhere were and are probably inevitable given the ongoing and expanding Russian "leasing" and/or other control of ports including Sevastopol, part of the ever-expanding spectrum of exigencies that offer inexorable opportunities to further exercise and perfect a decidedly idiosyncratic reading of the international rights to self-defense.

Although all segments of the book are valuable in delineating the Russian machinations and explanations often after the fact with their purported supporting legalities, Terry has done an equally articulate job in his longest and shortest chapters discussing the situations in Czechoslovakia in 1968 and Lithuania in 1990, respectively.

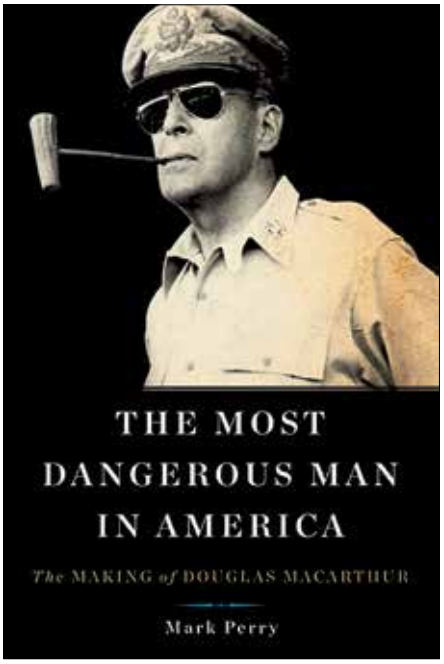
In the former instance, having obvious problems with but not altering its basic premises from the earlier Hungarian intervention episode, Russian justifications for its behavior in Czechoslovakia would eventually run a legal gamut, none with permanent potent efficacy. Terry's detailed explanation of how that evolved both factually and legally illuminates not only the specifics but also the nature of the Russian thought process.

As for the discussion relating to Lithuania, Terry notes that as one of the 14 Soviet Republics and autonomous regions to make the claim of independence from Moscow under "perestroika" in March 1990, the Baltic states most clearly met the criteria for self-determination established by international law affirmed by many including the then–Soviet Union, but that did not deter repeated threats and actions to the contrary. The decades-long struggle of Lithuania, although unique, illustrates a conundrum in international law, the weighing of protections for states versus peoples, and not exclusively in the realm of human rights.

In finite examples, Dr. Terry has demonstrated that Russia may now call itself a democracy, but unlike a rose which by any other name may smell as sweet, an oligarchy by any other name does not expand a leadership to more than merely a few. The individual country "crises" described herein are not all inclusive, of course, but as Terry sums up, provide a realistic guide for assessing the overall Russian approach to international legal commitments.

It is easy to concur with the foreword by eminent scholar John Norton Moore that "this is not a quick survey of Soviet/Russian uses of force, but rather an extraordinarily deep presentation and analysis of each. This important book also has crucial insights into the future of United States/Russian foreign relations. It is a must-read for those focused on international relations." **JFQ**

Alice A. Booher, JD, is a former Foreign Service Reserve Officer and Counsel in the Department of Veterans Affairs, Board of Veterans Appeals (1969–2011).



The Most Dangerous Man in America: The Making of Douglas MacArthur

By Mark Perry
Basic Books, 2014
380 pp. $29.99
ISBN 978-0465013289

Reviewed by Francis P. Sempa

Douglas MacArthur and Franklin Roosevelt first met in 1916 when both were involved in planning prewar mobilization for the Woodrow Wilson administration. Two years later, MacArthur was commanding the Rainbow Division in France where he earned seven Silver Stars for courage and bravery in leading his troops in battle against the Germans, while Roosevelt was serving as President Wilson's assistant Secretary of the Navy. When Roosevelt became President in 1933, MacArthur was the Army's chief of staff (having been appointed by President Herbert Hoover). Roosevelt, mainly for political reasons, extended MacArthur's term as Army chief of staff, but the two repeatedly clashed over budget matters. During World War II, Roosevelt as commander in chief selected MacArthur to lead the U.S. war effort in the Southwest Pacific.

The story of this fascinating relationship between two of the giants of the 20th century is the subject of Mark Perry's book. The title comes from a remark Roosevelt reportedly made to one of his aides early in his Presidency. When the aide suggested that Louisiana's Senator Huey Long was the most dangerous man in America, Roosevelt said no, Douglas MacArthur was. Perry credits Roosevelt with "taming" MacArthur's worst instincts and characteristics and skillfully using this most talented commander to help win the war in the Pacific.

Perry's book covers familiar ground: MacArthur's early defeats in the Philippines, his daring escape to Australia and famous pledge to return to liberate the Philippines, his frequent clashes with Washington and the Navy over war strategy and the allocation of resources, and his innovative strategy during the Southwest Pacific campaign where he brilliantly used land, sea, and air forces jointly to bypass Japanese strongholds during the New Guinea campaign.

Perry describes in great detail the formulation and implementation of MacArthur's Southwest Pacific strategy. From the defense of Australia and Port Moresby to the New Guinea offensive, and on to the recapture of the Philippines, Perry shows MacArthur at his best—waging a war of maneuver where possible that integrated all aspects of military power to achieve relatively economical (in terms of human costs) victories. It involved, writes Perry, "a series of combined arms operations involving dozens of ships, hundreds of aircraft, and tens of thousands of soldiers, whose movements would be coordinated over thousands of miles of ocean" (p. 230). In Operation *Cartwheel*, which focused on eliminating the Japanese stronghold of Rabaul, MacArthur, in Perry's judgment, "coordinated the most successful air, land, and sea campaign in the history of warfare" (p. 354).

MacArthur's success was due in part to his selection of and his reliance on first-rate subordinate commanders, such as the Airman George Kenney, Admiral

Thomas Kinkaid, and infantry General Walter Krueger, as well as his willingness to work with key naval commanders such as Chester Nimitz, William Halsey, and Raymond Spruance despite intense inter-Service rivalries. Perry also describes MacArthur's relationships with other key wartime figures, including George Marshall, Dwight Eisenhower, Secretary of War Henry Stimson, and various Australian and Filipino politicians.

MacArthur, of course, had his shortcomings and character flaws. He was arrogant, vain, and sometimes petty and vindictive. He viewed those in Washington who denied him resources or disagreed with his strategies as enemies. He frequently stretched the truth or outright lied about the status of battles (characterizing hard fought battles as "mopping-up operations") to vindicate his command decisions and receive adulatory media coverage. The Philippines campaign, for example, was far more costly than he predicted or would later admit; it degenerated into a bloody war of attrition that Perry describes in all its gruesome detail. But MacArthur was also incredibly courageous and brave, and was arguably the most brilliant military commander of World War II.

Roosevelt, a talented but deeply flawed man himself, to his credit recognized that MacArthur's strengths outweighed his flaws and weaknesses. Despite a personal animosity between these two leaders that stretched back to MacArthur's days as Army chief of staff, during the war both men usually put the country's interests first. Their relationship, Perry writes, "defined the war in the Pacific" (p. 355).

Perry's book is a welcome reevaluation of one of our nation's greatest and controversial military commanders and his relationship with his wartime commander in chief during the most momentous war in history. It provides valuable lessons on military leadership, inter-Service rivalries, civilian-military relations, and most important, the strategic benefits of joint operations. **JFQ**

Francis P. Sempa, an Assistant U.S. Attorney for the Middle District of Pennsylvania, is the author of *Geopolitics: From the Cold War to the 21st Century* (Transaction, 2007) and *America's Global Role: Essays and Reviews on National Security, Geopolitics and War* (University Press of America, 2009).

KC-135 Stratotanker assigned to 465th Air Refueling Squadron, 507th Air Refueling Wing, delivers fuel to F/A-18F Super Hornet assigned to Black Knights of Strike Fighter Squadron 154 supporting Rim of the Pacific 2010 exercises (U.S. Air Force/Kamaile O. Long)

The Way Ahead for Joint Operations and Planning Doctrine

By Rick Rowlett, Carl A. Young, Alan F. Mangan, and Steven M. Townsend

Two of joint doctrine's keystone[1] joint publications (JPs) have entered the window for revision—JP 3-0, *Joint Operations*, and JP 5-0, *Joint Operation Planning*. Both publications received comprehensive assessments in 2014, which generated a wide variety of recommended changes from combatant commands (CCMD), the Services, National Guard Bureau, Defense agencies, and the Joint Staff. This article describes the more significant of these.

Rick Rowlett is Lead Joint Doctrine Integrator in the Joint Doctrine Analysis Division at the Joint Chiefs of Staff (JCS) DJ7. Lieutenant Colonel Carl A. Young, USA, is Chief of the Plans Policy Branch in the Joint Operational War Plans Division (JOWPD) at the JCS DJ5. Alan F. Mangan is a War Plans Policy Analyst in the JOWPD JCS DJ5. Steven M. Townsend is a War Plans Policy Analyst in the JOWPD JCS DJ5.

JP 3-0: A Brief History

JP 3-0 (August 11, 2011) is the latest in a series of keystone JPs to address joint operations. JP 3-0 began as a January 1990 "test publication" titled *Doctrine for Unified and Joint Operations*.[2] General Colin Powell, then Chairman of the Joint Chiefs of Staff (CJCS), approved the first official version of JP 3-0 in 1993. It codified agreements that had been reached among the Joint Chiefs on a number of contentious aspects of joint operations.[3] In 1995,

General John Shalikashvili, General Powell's successor,[4] issued JP 3-0 with the Joint Doctrine Professional Library Desk Set,[5] which was made available on the Internet to increase access to and understanding of joint doctrine. Since then, the joint doctrine development community has revised JP 3-0 in 2001, 2006, and 2011. There also was a Change 1 in 2008 to ensure continuity with JP 1, and a Change 2 in 2010 to incorporate text on cyberspace and cyberspace operations.

What's Next? As a keystone publication, JP 3-0 has a symbiotic relationship with other publications in the joint doctrine hierarchy. JP 3-0 establishes (and is the authoritative source for) fundamental constructs with which other JPs must be consistent. Examples include the 12 principles of joint operations (appendix A of JP 3-0) and six joint functions (chapter III), as well as definitions for the terms *joint force*, *commander's intent*, and *operational art*. Similarly, other topic-focused JPs, such as JP 3-60, *Joint Targeting*, establish authoritative models and terms that influence the content of JP 3-0 and others. It is a challenge for JP authors to limit redundancy while sharing relevant material across joint publications. The joint community should see this challenge play out during the next year or so as authors of JPs 3-0, 5-0, and 3-20 (*Security Cooperation*) collaborate to achieve a balanced treatment of security cooperation, a topic sourced to JP 3-20 that affects both keystone JPs and others. The joint community can expect to see the following notable changes in the first draft of JP 3-0.

Security cooperation continuity across JP 3-0, JP 5-0, and JP 3-20 on the topic of security cooperation (SC) is one of the important issues that emerged during the JP 3-0 assessment and in events such as the semi-annual Joint Doctrine Planning Conference. JP 3-22, *Foreign Internal Defense*, is the current authoritative source for joint doctrine on SC, but JP 3-20 will assume this role when approved in late 2015. Joint Doctrine Planning Conference voting members approved development of a security cooperation JP to address the lack of understanding of SC, its relevance, and its relationship to activities such as security force assistance and foreign internal defense.

JP 3-0 currently covers security cooperation[6] primarily in context of low-range military operations, which focus on military engagement, security cooperation, and deterrence.[7] Both JP 3-0 and JP 5-0 describe SC as it relates to the notional phases of a joint operation.[8] Responses to the JP 3-0 assessment, supported by findings in the *Decade of War, Volume I* study[9] and various exercise observations, are sufficient to conclude that a more comprehensive discussion of SC is necessary. A new JP 3-20 should provide this discussion, and perhaps a revised definition. Consistent with JP 3-20, JP 3-0 will clarify the role of security cooperation with respect to the range of military operations, and JP 5-0 will cover SC in the context of theater campaign planning.

Security cooperation and a related topic, stability operations,[10] overlap in the general context of promoting a stable environment in a combatant commander's (CCDR's) area of responsibility (AOR). However, JP 3-0 does not address SC in sufficient detail with respect to its relationship to stability operations.[11] In a broad context, both SC and stability operations consist of activities that help maintain or improve stability consistent with U.S. objectives. Security cooperation, occasionally referenced informally as Phase Zero activities, is a central component of the CCDR's theater campaign plan. Security cooperation activities occur constantly within a CCDR's broader AOR, even if circumstances during more intense operations preclude these activities in a designated joint operations area. Stability operations, such as emergency infrastructure reconstruction, can occur in Phase Zero ("Shape"), but are not SC activities. While the magnitude of stability operations in a joint operations area will increase and decrease through the phases in many operations, security cooperation activities should remain relatively constant elsewhere in the AOR.[12] In addition to JPs 3-0, 3-20, and 5-0, JP 3-07, *Stability Operations*, is part of the solution to achieve clear and balanced doctrinal coverage of the security cooperation and stability operations relationship.

Assessment. In the context of gauging a military force's effectiveness during operations, the 2001 JP 3-0 focused on combat assessment. This is a tactical-level assessment of battle damage and munitions effectiveness that generates re-attack recommendations and supports targeting decisions. JP 3-0 retained combat assessment in 2006, and expanded the assessment discussion to the operational level through emphasis on creating desired effects and use of measures of effectiveness (MOEs) and measures of performance (MOPs). The 2006 JP 5-0 contained a closely related assessment discussion based on JP 3-0, and with slightly more detail. In 2011, the balance of doctrine on assessment shifted significantly from JP 3-0 to JP 5-0 (as described later in this article).

Joint force feedback generated a number of comments on the term *assessment* and the topic's treatment in joint doctrine. In particular, U.S. Central Command requested an extensive expansion of joint doctrine's assessment coverage. Assessment is a continuous process that measures the overall effectiveness of employing joint force capabilities during military operations by determining progress toward accomplishing tasks, creating conditions, and achieving objectives.[13] The main theme of feedback comments is that JP 3-0 should provide more detail on assessment and clarify a misunderstanding across CCMDs regarding who is responsible for developing an assessment plan during joint operation planning. Moreover, some commenters believe the discussion on developing MOEs and MOPs does not adequately address the challenge of developing an assessment plan that will help guide decisions and identify opportunities and risks during execution. Although the comments have merit, JP 3-0 is only part of the solution. JP 3-0 will provide a revised definition and an overview of assessment, while JP 5-0 will be the authoritative source for most of the keystone-level assessment doctrine.

Concepts. Approved concepts provide important potential sources of new ideas

Army paratroopers wait to perform personnel airdrop mission during joint operational access exercise, Fort Bragg, June 2011 (U.S. Air Force/Asha Harris)

that can improve joint doctrine. In 2011, JP 3-0 incorporated common operating precepts from the January 15, 2009, Capstone Concept for Joint Operations (CCJO).[14] The 10 precepts underlie successful joint operations and supplement the 12 principles of joint operations. The precepts flow logically from the broad challenges in the strategic environment to the specific conditions, circumstances, and influences in a joint force commander's operational environment.[15]

The Chairman of the Joint Chiefs of Staff approved the latest *Capstone Concept for Joint Operations: Joint Force 2020* in 2012.[16] It proposes an approach called globally integrated operations, which focuses on globally postured joint force elements that can combine quickly with each other and inter-organizational partners to integrate capabilities fluidly across domains, echelons, geographic boundaries, and organizational affiliations. Essential to realizing the CCJO's globally integrated operations is the projection of power despite antiaccess and area-denial challenges.[17]

The Joint Operational Access Concept (JOAC)[18] focuses on the ability to overcome these challenges and project military force into an operational area with sufficient freedom of action to accomplish the mission. Implementing the JOAC currently is a comprehensive, multiyear effort managed by the Joint Staff Joint Force Development Directorate (J7) in conjunction with other Joint Staff directorates, CCMDs, Services, and Defense agencies. The joint doctrine contribution to the effort involves potential changes between now and 2020 to at least 35 JPs that span all joint functions. The current JP 3-0 mentions the importance of access to operational areas, but readers should expect to see an expansion of this discussion during the upcoming revision, beginning with emphasis on SC activities that can set the peacetime conditions for gaining and maintaining operational access as the JOAC envisions.

Content Reorganization. In addition to changes highlighted above, content organization adjustments will be evident in the JP 3-0 first draft. These focus on redistributing major topics in the current chapter V, "Joint Operations across the Range of Military Operations," to provide a more logical sequence and improve readability of the 65-page chapter. A new chapter V, "Joint Operations across the Conflict Continuum," will discuss the range of military operations; types of military operations; the phasing construct (current figure V-3 and related text); the balance of offense, defense, and stability operations (current figure V-4 and related text); and linear and nonlinear operations. The reorganization will shift the remainder of the current chapter V information into three chapters: chapter VI, "Military Engagement, Security Cooperation, and Deterrence"; chapter VII, "Crisis Response and Limited Contingency Operations"; and chapter VIII, "Major Operations and Campaigns." The new

Tandem jumpers from Army Golden Knights Parachute Team free fall after jumping from Air Force Special Operations Command CV-22 Osprey over MacDill Air Force Base (DOD)

chapter V will group related topics and position them to provide a better introduction to the three subsequent chapters.

Conclusion. The JP 3-0 revision will be informed by the latest information available from joint community feedback, various lessons learned and best practices from current operations, and relevant, validated constructs identified during assessment of approved joint concepts. The revision will also focus on achieving continuity and appropriate balance of related topics like security cooperation in publications such as JP 3-20 and JP 5-0. The objective is to ensure that, when approved in 2016, the revised keystone joint operations publication remains a relevant and current doctrinal foundation for all other JPs.

JP 5-0: A Brief History

The Joint Doctrine Professional Library Desk Set also included the 1995 JP 5-0, *Doctrine for Planning Joint Operations.* This version was substantially different in form from the current JP 5-0, and more strategically focused. When published, the 1995 JP 5-0 was the keystone planning publication in a series that included seven additional planning JPs.[19] However, four of these were Joint Operation Planning and Execution System (JOPES) JPs that the Joint Staff J5 was updating and republishing as CJCS instructions. A fifth provided information on JOPES automated data processing support.

Two other JPs in the 1995 joint planning series supported JP 5-0. JP 5-00.1, *Joint Tactics, Techniques, and Procedures for Joint Campaign Planning*, was revised in 2002 as *Joint Doctrine for Campaign Planning*, and was then merged into the December 26, 2006, revision of JP 5-0. JP 5-00.2, *Joint Task Force Planning Guidance and Procedures*, was revised in 1999. During the 2007 revision, it was renumbered and renamed JP 3-33, *Joint Task Force Headquarters*, leaving JP 5-0 as the only remaining planning-focused joint publication.

What's Next? The 2014 formal assessment and analysis indicated that the current JP 5-0 discussion of operational-level planning is largely sufficient. The joint community should not expect to see significant changes in chapter II, "Strategic Direction and Joint Operation Planning"; chapter III, "Operational Art and Operational Design"; and chapter IV, "Joint Operation Planning Process." However, the analysis also concluded that, while the primary operational-level focus (planning for contingencies) of the current publication is sound, major gaps exist in doctrine for theater- and national-strategic planning. Additionally, discontinuity remains between contingency plans, theater strategic planning,

and the strategic decisionmaking process at the Department of Defense (DOD) level. The current JP 5-0 does not address development of a CCDR's theater campaign plan and the nesting of contingency plans and relevant country plans, nor does it address the role of planning in support of national decisions. The joint community can expect to see the following notable changes in the first draft of JP 5-0.

Scope. First, the title of JP 5-0 will change from "Joint Operation Planning" to "Joint Planning" to reflect the expanded scope of the publication. Chapter I, "Role of Joint Planning," will be expanded to address the different requirements placed on planning at the national decisionmaking level (national approach) and the requirements of the joint force to execute operations when directed by the President or Secretary of Defense. This chapter will also introduce the campaign as the tool that DOD uses to translate national strategic guidance into ongoing activities to achieve national objectives. This will include a discussion of using "threat sets" in planning. Briefly, threat sets consider the whole of a military problem, particularly the interrelated planning tasks of multiple CCMDs that cross the gaps and seams between geographic and functional commands and link interrelated threats to response options in the context of continuous risk assessment under the direction of a supported commander. Threat sets define the priority effort of a complex contingency problem and help define the supporting and supported command relationships across CCMDs.

The most significant change is the addition of a new chapter titled "Campaign Planning." This chapter will assist CCMD planners in developing their command's campaign and using it to link theater operations to national strategy and CCMD campaign plans to subordinate contingency plans. The chapter will emphasize campaign assessments to address concerns about how assessments are conducted, their purpose in measuring success of the campaign, and the link between campaigns and resourcing.

Role of Joint Planning. Added to chapter I, "Role of Joint Planning," is a discussion on the differing perspectives of planning between the CCMDs and national-level decisionmakers. Planners face the challenge of developing specific plans to address identified threat sets, while a national approach to the issues has not been fully decided. The result is that national-level decisionmakers want to consider a wide range of options (across the diplomatic, informational, military, and economic instruments of national power, with associated risk assessments), and are often cautious about committing to a specific approach and providing specific guidance too quickly before a crisis occurs. Conversely, joint force planners require specific guidance (and decisions on assumptions such as timing, expected force levels, and coalition support) to conduct in-depth analysis to provide the requisite level of assessment to inform the decision process. This tension allows senior decisionmakers to preserve flexibility while getting detailed information on a wide range of possible options. In contrast, joint planners at and below the CCMD develop specific (and often narrow) military solution sets to determine requirements and risk. The revision of JP 5-0 will identify processes to help bridge this gap and satisfy the information needs of both sides.

Second, national-level guidance is often broad and unconstrained. The processes identified in JP 5-0 will help CCDRs and their staffs develop strategy and plan campaigns to bridge the gap between national policy and joint operation planning. The description of the theater campaign plan as the top-level CCMD plan links national strategy to daily activities, which are directed in the CCDR's campaign plans and provide a foundation for developing contingency plans.

Campaign Planning and the Purpose of the Campaign. The update to JP 5-0 will include a new chapter titled "Strategy and Campaign Development" in addition to the existing chapter on operational planning. This chapter will link CCMD campaign plans to the CCMD strategy and its operation and contingency plans. The CCMD campaigns serve as the DOD translation of national strategic guidance into actionable and operational-level activities within the resources available. The CCDR assesses the environment and the command's ability to influence change within the guidance, authorities, and available resources. This enables senior leader strategic discussions linking realistic and achievable objectives and associated risks to national objectives across a wide range of options. This chapter will introduce several new concepts:

- CCDRs document the full scope of their campaigns in a comprehensive set of plans that includes the overarching theater or functional campaign plan, all subordinate campaign and supporting, posture or master, security cooperation, country, and contingency plans.[20]
- The role of Phase Zero will be examined. Foundational activities outlined in the theater campaign plan, such as those typical of security cooperation, are conducted routinely throughout the campaign. They have both shaping and deterrent effects that support contingency planning. Although some campaign activities can have deterrent effects, Phase I ("Deter") operations are outside the scope of a campaign's routine security cooperation activities, so they remain in contingency plans and are executed on order.
- Since the campaign seeks to achieve nationally directed objectives, the term *steady state* is discouraged. The campaign seeks to achieve measurable objectives that improve the operational environment's alignment with the CCDR's strategic or theater objectives in support of national objectives.
- Campaigns seek to set conditions within the operational environment to achieve nationally directed objectives. They are tied to contingency plans in that the campaign serves to prevent, prepare for, or mitigate the impact of a crisis that could require implementation of a contingency plan. Therefore, whether a CCDR must execute a contingency plan

often depends on the success of the CCMD's campaign to maintain the desired conditions in the operational environment. Planners' assessment of the campaign assists in developing information on planning assumptions.

- Once executed, a contingency plan becomes an element of the campaign and must be "normalized" within the campaign. Anything that happens within an operation affects the environment and may require changes to the campaign. CCDRs must adjust resources and activities across their areas of responsibility to respond to new operations, as they affect the resources, campaign environment, and the effects of other activities.
- Campaign planning, therefore, is a seamless approach that includes strategic considerations about options presented to senior military and civilian leaders, while simultaneously preparing for changes in the environment.

A significant change to the proposed campaign planning construct is that campaign and contingency planning will occur within the restrictions of existing resources. This "resource-informed" planning, as directed in the 2015 *Guidance for the Employment of the Force* and 2015 *Joint Strategic Capabilities Plan*, requires the planner to assess the objectives of the campaign, the likelihood of contingencies, and balance the forces, posture, fiscal resources, materiel, and authorities that are available and have been apportioned to prepare a successful plan. DOD policy directs that plans not serve as CCDR demand signals.

Assessment. The current discussion on assessment expands to address assessments that support campaign planning. The primary topics of discussion at the strategic level center on the CCDR's assessment of the environment, the operation, and risk associated with the campaign and any operation.

The current JP 5-0 addresses assessments as an element of the plan (assessments are included in the plan to evaluate the effectiveness of that plan in achieving its objectives). The expanded section will integrate additional details from Joint Doctrine Note 1-14, "Operation Assessment," with a focus on how assessments aid the decisionmaking process and are used to monitor execution and adjust the campaign (and contingency plans) to improve success. Since campaigns are ongoing, assessments must be continuous and should support the development of the subsequent campaign plan. Assessments help to determine the effectiveness and efficiency of the programs in progress and those programmed in the current fiscal, force management, and training cycles. As planning occurs, ongoing assessments provide feedback and information resulting from changes in the environment (due to previously scheduled activities or ongoing operations) that may require changes in the plans currently in execution or those intended for future implementation. Continuous assessment of the campaign informs contingency planning because the assessment might validate contingency plan assumptions as well as identify changes in the environment under which a contingency is executed.

CCDRs include the assessment plan and results of ongoing assessments in the review process with national leadership. This information provides the CCDR talking points to identify national-level decisions or issues that senior leaders must address to achieve strategic objectives. Assessments identify assumptions, risks, decision points, support required from interagency and multinational partners, and other factors that either validate current progress or necessitate changes to campaign and contingency plans and ongoing operations.

Risk. The current version of JP 5-0 identifies risk as a topic of discussion and critical to the decisionmaking process, but does not provide support to help the planner identify, categorize, and discuss risk. The revised JP 5-0 will contain a new appendix on risk, helping planners identify and manage risk throughout the planning process. Improved risk discussions will improve national-level discussions and decisionmaking. Risk discussion will center on risk to the force (for example, "Do I have the correct force, ready enough?" "Are my casualty estimates acceptable?"), risk to mission ("What are the impacts if I get fewer forces, delayed timing"), risk to other missions ("What must I divert from other missions and how will that affect my ability to accomplish them?"), and the impact of political risk ("How will operations affect public opinion, local opinion, allied opinion, and adversaries?").

Content Reorganization. In addition to the major changes noted above, several other changes are proposed for the update. The in-progress review discussion and figure I-1, "Adaptive Planning Review and Approval Process," will move to chapter V, "Joint Planning Process," in line with its logical sequence in the process. The discussion on inter-organizational and multinational planning, previously split into two different areas in chapter II, will consolidate into one section. As mentioned, chapter III will be a new one that covers strategy and campaign development. Current chapters III and IV become chapters IV and V in the update, with similar structures as the current chapters. Two new chapters are added at the end: chapter VI covers transition to execution, to better tie in to JP 3-0, and chapter VII addresses assessments. In the appendices, the "Plan Format" appendix will be removed to reduce the size and avoid conflicts with the formats published in the CJCSM 3130 series manuals, which are updated more frequently. The appendices on flexible deterrent options and flexible response options will be combined. Two new appendices will address risk identification and management and theater posture plans.

Conclusion. Campaigns translate national-level policy and guidance into theater-strategic and operational-level activities conducted to further U.S. interests to prevent, prepare for, or mitigate the impact of a crisis or contingency. The new JP 5-0 will provide a doctrinal basis for planners at the CCMDs, Joint Staff, Service component commands, and Services to address planning for those operations and activities that DOD conducts on a continuing basis.

U.S. Army AH-64D Apache helicopter takes off from Afloat Forward Staging Base (Interim) USS *Ponce* during exercise, November 2012 (U.S. Navy/Jon Rasmussen)

The 2015 JP 5-0 update enables planners to better prepare their leadership for discussions in the strategic decision space at the national and theater levels. Campaign plans operationalize national-level guidance into daily activities that shape and influence the strategic environment to prevent, prepare for, or mitigate the effects of contingencies. The 2016 JP 5-0 will address this perspective of CCMD campaigns and campaign plans. **JFQ**

Notes

[1] Keystone joint publications (JPs) are the six functionally oriented doctrine publications: JPs 1-0, *Joint Personnel Support* (Washington, DC: The Joint Staff, October 24, 2011); JP 2-0, *Joint Intelligence* (Washington, DC: The Joint Staff, October 22, 2013); JP 3-0, *Joint Operations* (Washington, DC: The Joint Staff, August 11, 2011); JP 4-0, *Joint Logistics* (Washington, DC: The Joint Staff, October 16, 2013); JP 5-0, *Joint Operation Planning* (Washington, DC: The Joint Staff, August 11, 2011); and JP 6-0, *Joint Communications System* (Washington, DC: The Joint Staff, June 10, 2010) are directly under the capstone JP 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 25, 2013). All other JPs are grouped under the keystones.

[2] Joint Chiefs of Staff Publication 3-0, *Doctrine for Unified and Joint Operations* (Washington, DC: The Joint Staff, January 1990).

[3] On November 23, 1992, General Colin Powell signed a memorandum (CM-1502-92, Subject: A Doctrinal Statement of Selected Joint Operational Concepts) that formalized an accompanying "doctrinal paper" titled *A Doctrinal Statement of Selected Joint Operational Concepts.* This document represented agreement among the Joint Chiefs of Staff on selected aspects of joint operations, and was intended to guide development of the 1993 JP 3-0 as well as JP 3-03, *Doctrine for Joint Interdiction Operations*; and JP 3-09, *Doctrine for Joint Fire Support.*

[4] Admiral David Jeremiah served as acting Chairman for 23 days between Generals Powell and John Shalikashvili.

[5] The desk set also contained other keystone JPs, a CD-ROM, and a VHS video.

[6] JP 3-22, *Foreign Internal Defense* (Washington, DC: The Joint Staff, July 12, 2010), x, defines *security cooperation* as Department of Defense "interactions with foreign defense establishments to build defense relationships that promote specific US security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to a host nation."

[7] JP 3-0. For an introduction to the range of military operations, see paragraph 3 on I-4. For an expanded discussion of military engagement, security cooperation, and deterrence, see paragraph 4 on V-9.

[8] Ibid. See figure V-3, "Notional Operation Plan Phases versus Level of Military Effort," as well as the discussion of the phasing model that begins on V-7.

[9] Joint and Coalition Operational Analysis (JCOA), Joint Staff J7, *Decade of War Volume I: Enduring Lessons from the Past Decade of War* (Suffolk, VA: JCOA, June 15, 2012). In particular, see "Lesson Nine: Host Nation Partnering," 32.

[10] JP 3-0, V-4, defines *stability operations* as "an umbrella term for various military missions, tasks, and activities conducted outside

the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and to provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief."

[11] JP 3-07, *Stability Operations* (Washington, DC: The Joint Staff, September 29, 2011), provides details on this topic.

[12] Ibid. See figure V-4, which describes the notional balance of offense, defense, and stability operations in a single joint operation.

[13] Ibid. Paraphrased selectively from the glossary definition, GL-5.

[14] *Capstone Concept for Joint Operations, Version 3.0* (Washington, DC: Department of Defense, January 15, 2009). See paragraph 6 beginning on 21.

[15] JP 3-0, figure I-2. Additionally, the individual precepts are located throughout JP 3-0 where they amplify related text. See paragraph 5 on I-8 for an example.

[16] *Capstone Concept for Joint Operations: Joint Force 2020* (Washington, DC: Joint Chiefs of Staff, September 10, 2012).

[17] *Joint Operational Access Concept (JOAC), Version 1.0* (Washington, DC: Department of Defense, January 17, 2012), 40. *Antiaccess* refers to those capabilities, usually long range, designed to prevent an advancing enemy from entering an operational area. *Area-denial* capabilities are those usually of shorter range, designed not to keep the enemy out but to limit his freedom of action within the operational area.

[18] Ibid.

[19] JP 5-0, *Doctrine for Planning Joint Operations* (Washington, DC: The Joint Staff, April 13, 1995). Figure III-1, "Joint Publication 5-0 Series Hierarchy," shows the eight JPs in the JP 5-0 series.

[20] While a combatant command (CCMD) may have multiple campaign plans or ongoing campaigns, it has only one theater or functional campaign plan (TCP/FCP), to and of which all of its other plans (campaign, support, operation, posture, master, country, or contingency) are subordinate and a part. Through the TCP/FCP the CCMD holistically plans and executes actions to achieve the national objectives for the theater. Subordinate campaign plans allow joint force commanders to focus on specific regions or problem sets within the CCMD area of operation, while the combatant commander ensures that all plans are coordinated and actions synchronized within the theater.

Joint Publications (JPs) Under Revision (to be signed within 6 months)

JP 1-0, *Joint Personnel Support*

JP 1-04, *Legal Support to Military Operations*

JP 3-05.1, *Unconventional Warfare*

JP 3-13.3, *Operations Security*

JP 3-15, *Barriers, Obstacles, and Mine Warfare*

JP 3-50, *Personnel Recovery*

JP 3-61, *Public Affairs*

JP 3-68, *Noncombatant Evacuation Operations*

JP 4-01.2, *Sealift Support to Joint Operations*

JP 4-01.5, *Joint Terminal Operations*

JP 6-0, *Joint Communications System*

JPs Revised (signed within last 6 months)

JP 3-02.1, *Amphibious Embarkation and Debarkation* (November 25, 2014)

JP 3-09, *Joint Fire Support* (December 12, 2014)

JP 3-09.3, *Close Air Support* (November 25, 2014)

JP 3-10, *Joint Security Operations in Theater* (November 13, 2014)

JP 3-12(R), *Cyberspace Operations* (published October 21, 2014, retained original signature date of February 5, 2013)

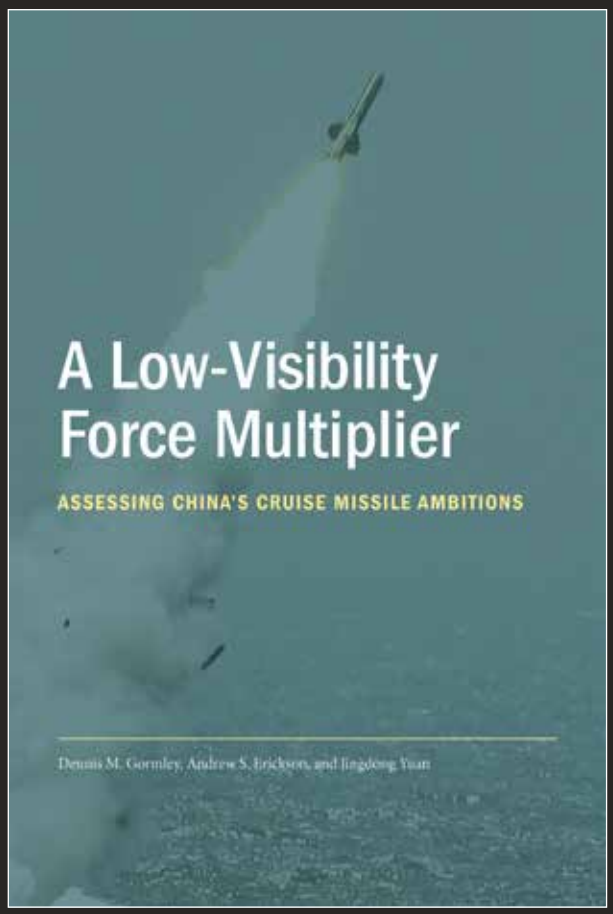
JP 3-13.2, *Military Information Support Operations* (November 21, 2014)

JP 3-26, *Counterterrorism* (October 24, 2014)

JP 3-40, *Countering Weapons of Mass Destruction* (October 31, 2014)

JP 3-52, *Joint Airspace Control* (November 13, 2014)

JP 3-63, *Detainee Operations* (November 13, 2014)



NEW from NDU Press

A Low-Visibility Force Multiplier:
Assessing China's Cruise Missile Ambitions
By Dennis M. Gormley, Andrew S. Erickson, and Jingdong Yuan

China's military modernization includes ambitious efforts to develop antiaccess/area-denial (A2/AD) capabilities to deter intervention by outside powers. Highly accurate and lethal antiship cruise missiles and land-attack cruise missiles carried by a range of ground, naval, and air platforms are an integral part of this counter-intervention strategy. This comprehensive study combines technical and military analysis with an extensive array of Chinese language sources to analyze the challenges Chinese cruise missiles pose for the U.S. military in the Western Pacific.

"Cruise missiles are key weapons in China's A2/AD arsenal, providing a lethal precision-strike capability against naval ships and land-based targets. The authors use hundreds of Chinese language sources and expertise on cruise missile technology to assess China's progress in acquiring and developing advanced antiship and land-attack cruise missiles and to consider how the People's Liberation Army might employ these weapons in a conflict. Essential reading for those who want to understand the challenges China's military modernization poses to the United States and its allies."

—**David A. Deptula**, Lieutenant General, USAF (Ret.),
Senior Military Scholar, Center for Character and Leadership
Development, U.S. Air Force Academy

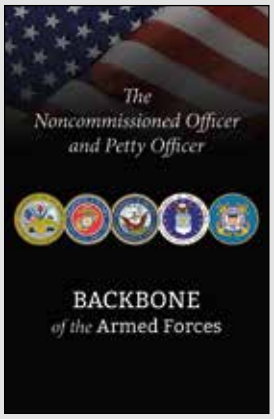
"This volume is a major contribution to our understanding of Chinese military modernization. Although China's ballistic missile programs have garnered considerable attention, the authors remind us that Beijing's investment in cruise missiles may yield equally consequential results."

—**Thomas G. Mahnken**, Jerome E. Levy Chair of
Economic Geography and National Security, U.S. Naval War College

"This book provides an excellent primer on the growing challenge of Chinese cruise missiles. It shows how antiship and land-attack cruise missiles complicate U.S. efforts to counter China's expanding A2/AD capabilities and are becoming a global proliferation threat. The authors also demonstrate just how much progress China has made in modernizing and upgrading its defense industry, to the point of being able to develop and produce world-class offensive weapons systems such as land-attack cruise missiles. This book belongs on the shelves of every serious observer of China's growing military prowess."

—**Richard A. Bitzinger**, Coordinator, Military Transformations Program,
S. Rajaratnam School of International Studies, Singapore

Available online at ndupress.ndu.edu/Portals/68/Documents/Books/force-multiplier.pdf



The Noncommissioned Officer and Petty Officer: Backbone of the Armed Forces

NDU Press, 2013 • 176 pp.

A first of its kind, this book—of, by, and for noncommissioned officers and petty officers—is a comprehensive explanation of enlisted leaders across the United States Armed Forces. It balances with the Services' NCO/PO leadership manuals and complements *The Armed Forces Officer*, the latest edition of which was published by NDU Press in 2007. Written by a team of Active, Reserve, and retired enlisted leaders from the five Service branches, this book describes how NCOs/POs fit into an organization, centers them in the Profession of Arms, defines their dual roles of complementing the officer and enabling the force, and exposes their international engagement. As Chairman of the Joint Chiefs of Staff General Martin E. Dempsey writes in his foreword to the book, "We know noncommissioned officers and petty officers to have exceptional competence, professional character, and soldierly grit—they are exemplars of our Profession of Arms."

Aspirational and fulfilling, this book helps prepare young men and women who strive to become NCOs/POs, re-inspires currently serving enlisted leaders, and stimulates reflection by those who no longer wear the uniform. It also gives those who have never served a comprehensive understanding of who these exceptional men and women are, and why they are known as the "Backbone of the Armed Forces."

Have you checked out NDU Press online lately?

With 20,000 unique vistors each month, the NDU Press Web site is a great place to find information on new and upcoming articles, occasional papers, books, and other publications.

You can also find us on:

Facebook **Flickr**

Twitter **Pinterest**

Visit us online at: **http://ndupress.ndu.edu**

JFQ is available online at the Joint Electronic Library:
www.dtic.mil/doctrine/jfq/jfq.htm

JFQ
JOINT FORCE QUARTERLY
Published for the Chairman of the Joint Chiefs of Staff by National Defense University Press
National Defense University, Washington, DC
NDU Press